Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 647 - Abstract Algebra
Instructor: Dr.Victor Ostrik

Homework - Optional Problems
ID: 952091294
Term: Fall 2024
Due Date: End of fall term, 2024

Problem 1.6.7.
Let V be an infinite dimensional vector space. Show that the linear map $\iota_V : V \to V^{**}$ defined just before Exercise 1.2.8. is injective but not surjective.

Solution: We first prove that ι_V is injective. Let $v \in \ker(\iota_V)$, we have $f(v) = 0$ for every $f \in V^*$. We claim that $v = 0$. Assume the opposite. $\{v\}$ is linearly independent and can be extended to a basis for V. Define a linear functional $g \in V^*$ which sends v to 1 and sends any other base vectors to 0. This contradicts that $g(v) = 0$. Thus, $\ker(\iota_V) = 0$ and ι_V is injective.

Now we are going to prove that ι_V can never be surjective by show that $\dim V^*$ is strictly larger than $\dim V$ if V is infinite dimensional. Let X be a set of basis of V and since X is infinite, it must contain a countable subset, denoted by $\{e_n\}_{n\in\mathbb{N}}$. For each $a \in \mathbb{F}$, we define a functional $f_a : V \to \mathbb{F}$, $f_a(e_n) = a^n$ for all $n \in \mathbb{N}$ and f_a maps the basis in $X \setminus \{e_n\}_{n\in\mathbb{N}}$ to 0.
Claim: The set $\{f_a\}_{a\in\mathbb{F}} \subset V^*$ is linearly independent.
Proof: Assume the opposite. Then there exists different $a_1, \ldots, a_n \in \mathbb{F}$ and $c_1, \ldots, c^n \in \mathbb{F}$ such that

$$c_1 f_{a_1} + \cdots + c_n f_{a_n} = 0$$

and $c_1, \ldots, c_n$ are not all zero. Evaluate the above functional on $e_0, e_1, \ldots, e_m$ and we have

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^m & a_2^m & \cdots & a_n^m \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = 0$$

This function has a nonzero solution for $c_1, \ldots, c_n$, so we know that the determinant of

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^m & a_2^m & \cdots & a_n^m \end{pmatrix}$$

must be 0. But A is the transpose of Vandermonde matrix and $0 = \det A = \prod_{1\le i<j\le m}(a_j - a_i)$. Thus, there exist $1 \le i < j \le m$ such that $a_i = a_j$. This contradicts our assumption that $a_1, \ldots, a_n$ are different elements in $\mathbb{F}$. ■
We know that $\{f_a\}_{a\in\mathbb{F}}$ is linearly independent subset in V^* and can be extended to a basis of V^*, therefore, we know that $\dim V^* \ge |\mathbb{F}|$. By Exercise 1.6.5., $|V^*| = \max(|\mathbb{F}|, \dim V^*) = \dim V^*$. By Exercise 1.6.6., $|V^*| = \dim V^* > \dim V$, so $|V^*| > \max(|\mathbb{F}|, \dim V) = |V|$, it is impossible to have a surjective map from V to V^*.

Problem 2.4.6

For a commutative ring R, let $GL_n(R)$ be the group of all invertible $n \times n$ matrices with the entries in R with respect to the usual matrix multiplication. Given a homomorphism $f : R \to S$ of commutative rings, show that the map $GL_n(f) : GL_n(R) \to GL_n(S)$ obtained by applying f to all of the entries of an $n \times n$ matrix is actually a group homomorphism. Then verify that this defines a group scheme GL_n.

Solution: Let $M, N \in GL_n(R)$ be matrices with entries in R. Write $M = (a_{ij})_{1 \le i,j \le n}$ and $N = (b_{kl})_{1 \le k,l \le n}$. Then by matrices multiplication $(MN)_{ij} = \Sigma_{k=1}^{n} a_{ik} b_{kj}$. Apply $GL_n(f)$ and we get

$$\begin{aligned}(f(MN)) &= f((\Sigma_{k=1}^{n} a_{ik} b_{kj})_{1 \le i,j \le n}) \\ &= (\Sigma_{k=1}^{n} f(a_{ik}) f(b_{kj}))_{1 \le i,j \le n} \\ &= f((a_{ij})_{1 \le i,j \le n}) \cdot f((b_{kl})_{1 \le k,l \le n}) \\ &= f(M) \cdot f(N).\end{aligned}$$

The middle equality is because $f : R \to S$ is a ring homomorphism. This proves that $GL_n(f)$ is actually a group homomorphism. Next, we are going to show that GL_n is compatible with morphisms composition in **CRings**. Suppose $f : R \to S$ and $g : S \to T$ are morphisms between commutative rings. Let $M = (a_{ij})_{1 \le i,j \le n}$ be a $n \times n$ matrix with entries in R. Then for each $1 \le i, j \le n$, we have

$$(GL_n(g \circ f)(M))_{ij} = (g \circ f)(a_{ij}) = g(f(a_{ij})) = (GL_n(g) \circ GL_n(f)(M))_{ij}.$$

Let $id : R \to R$ be an identity morphism of a commutative ring R. Then $GL_n(id) : GL_n(R) \to GL_n(R)$ is also the identity morphism since for each entry of the matrix, it is the identity. Thus we can conclude that GL_n is a functor from **CRings** to **Groups**, which means that it is a group scheme.

Problem 2.4.9

Let **A**,**B** and **C** be categories. Use the interchange law to show that there is a bifunctor

$$\mathbf{Func}(\mathbf{B}, \mathbf{C}) \times \mathbf{Func}(\mathbf{A}, \mathbf{B}) \to \mathbf{Func}(\mathbf{A}, \mathbf{C})$$

mapping an object $(\mathscr{G}, \mathscr{F})$ to $\mathscr{G} \circ \mathscr{F}$ and a morphism (β, α) to $\beta \star \alpha$.

Solution: Write the bifunctor as T. Let $\mathscr{G} : \mathbf{B} \to \mathbf{C}$ and $\mathscr{F} : \mathbf{A} \to \mathbf{B}$ be two functors. Write $id_{\mathscr{F}}$ and $id_{\mathscr{G}}$ as the identity natural transformation of $\mathscr{F}$ and $\mathscr{G}$. Then $T(id_{\mathscr{G}}, id_{\mathscr{F}}) = id_{\mathscr{G}} \star id_{\mathscr{F}}$. For every object $X \in \operatorname{Ob} A$, by Exerise 2.4.7.(3), we have $(id_{\mathscr{G}} \star id_{\mathscr{F}})_X = (id_{\mathscr{G}}\mathscr{F})_X = \mathscr{G}\mathscr{F}X$. So $T(id_{\mathscr{G}}, id_{\mathscr{F}}) = id_{\mathscr{G} \circ \mathscr{F}}$.

Let $\mathscr{E}, \mathscr{F}, \mathscr{G} : \mathbf{A} \to \mathbf{B}$ and $\mathscr{H}, \mathscr{I}, \mathscr{J} : \mathbf{B} \to \mathbf{C}$ be functors, and $\alpha : \mathscr{E} \Rightarrow \mathscr{F}$, $\beta : \mathscr{F} \Rightarrow \mathscr{G}$, $\gamma : \mathscr{H} \Rightarrow \mathscr{I}$

and $\delta : \mathcal{I} \Rightarrow \mathcal{J}$ be natural transformations as the following diagram:

$$\begin{tikzcd}
\mathbf{C} & & \mathbf{B} \arrow[ll, bend right=50, "\mathcal{J}"'] \arrow[ll, "\mathcal{I}" description] \arrow[ll, bend left=50, "\mathcal{H}"] \arrow[ll, phantom, shift right=3, "\Uparrow\delta"] \arrow[ll, phantom, shift left=3, "\Uparrow\gamma"] & & \mathbf{A} \arrow[ll, bend right=50, "\mathcal{G}"'] \arrow[ll, "\mathcal{F}" description] \arrow[ll, bend left=50, "\mathcal{E}"] \arrow[ll, phantom, shift right=3, "\Uparrow\beta"] \arrow[ll, phantom, shift left=3, "\Uparrow\alpha"]
\end{tikzcd}$$

We know from Exercise 2.4.8. (The interchange law) that

$$T((\delta \circ \gamma), (\beta \circ \alpha)) = (\delta \circ \gamma) \star (\beta \circ \alpha) = (\delta \star \beta) \circ (\gamma \star \alpha) = T(\delta, \beta) \circ T(\gamma, \alpha).$$

This proves that T is a bifunctor.

Problem 3.3.6
If G is a finite group with an even number of elements, then the number of involutions in G is odd.

Solution: To prove that the number of involutions in G is odd, it is the same as showing that the number of elements in G which are not involutions is odd. Let $a \in G$ such that the order of a is larger than 2. We claim that $a \neq a^{-1}$. Indeed, if $a = a^{-1}$, then $a^2 = 1$, which means that a has order 2. A contradiction. Moreover, both a and a^{-1} has the same order as $(a^{-1})^n = 1$ if and only if $a^n = 1$. So the elements in G with order larger than 2 come in pairs, which means the number of them must be even. And the identity element has order 1. So the number of elements in G which are not involutions must be odd.

Problem 3.3.10
Let $H \leq G$ and $K \trianglelefteq G$. Show that $K \trianglelefteq HK \leq G$ and that the map $f : H \to HK/K, h \mapsto hK$ is surjective with the kernel $H \cap K$. Hence it induces an isomorphism $f : H/(H \cap K) \xrightarrow{\sim} HK/K$.

Solution:

1. $K \trianglelefteq HK \trianglelefteq G$
   We know that $HK = \{hk \,|\, h \in H,\, k \in K\}$. Given $k_1 \in K$, for every $h \in H$ and $k \in K$, since K is normal in G, we have $(hk)k_1(hk)^{-1} = hk \cdot k_1 \cdot k^{-1}h^{-1} = h(kk_1k^{-1})h^{-1} \in K$. Thus, $K \trianglelefteq HK$. Given $h_1k_1, h_2k_2 \in HK$, we have $h_1k_1h_2k_2 = (h_1h_2)(h_2^{-1}k_1h_2)k_2$, where $h_1h_2 \in H$ and $(h_2^{-1}k_1h_2)k_2 \in K$ as $K \trianglelefteq G$. This proves that $h_1k_1h_2k_2 \in HK$, meaning HK is a subgroup of G.

2. f is surjective and $\bar{f}$ is an isomorphism.
   We first show that for every $h \in H$ and $k_1, k_2 \in K$, hk_1 and hk_2 are in the same coset. Indeed, $hk_1(hk_2)^{-1} = hk_1k_2^{-1}h^{-1} \in K$. Therefore, for any coset $hK \in HK/K$, its preimage under f must contain h. This proves that f is surjective. Let $a \in H$. We have $f(a) = aK$. We know that $aK = K$ if and only if $a \in K$, which means $a \in \ker f$ if and only if $a \in H \cap K$. This proves that $\ker f = H \cap K$. By the first isomorphism theorem (Exercise 3.3.9.), we know that $\bar{f} : H/(H \cap K) \xrightarrow{\sim} HK/K$ is an isomorphism.

Problem 3.6.6
Show that $\mathbb{F}[x_1, \ldots, x_n]$ is an integral domain.

Solution: We prove this by induction on the number n of indeterminates. When $n = 1$, write the free $\mathbb{F}$-algebra as $\mathbb{F}[x]$, where the elements are just polynomials. Assume $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ where the leading term a_n, b_m are nonzero and we have $fg = 0$ for some $m, n \geq 0$. Then fg can be written as

$$0 = fg = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + (\sum_{i=0}^{k} a_ib_{k-i})x^k + \cdots + (\sum_{i=0}^{m+n} a_ib_{m+n-i})x^{m+n}.$$

This implies $\sum_{i=0}^{k} a_ib_{k-i} = 0$ for $k = 0, 1, \ldots, m + n$. A field is always an integral domain so we can see that

$$\begin{aligned} a_0b_0 &= 0 & &\Rightarrow a_0 = b_0 = 0 \\ a_2b_0 + a_1b_1 + a_0b_2 &= 0 \Rightarrow a_1b_1 = 0 & &\Rightarrow a_1 = b_1 = 0 \\ \sum_{i=0}^{4} a_ib_{4-i} &= 0 \Rightarrow a_2b_2 = 0 & &\Rightarrow a_2 = b_2 = 0 \\ &\cdots \end{aligned}$$

This proves that both $f = g = 0$.

Now assume $n \geq 2$ and we have prove that $\mathbb{F}[x_1, \ldots, x_{n-1}]$ is an integral domain. View the field $\mathbb{F}[x_1, \ldots, x_n]$ as a free $\mathbb{F}[x_1, \ldots, x_{n-1}]$-algebra. Let $f, g \in \mathbb{F}[x_1, \ldots, x_n]$. Write $f = p_0 + p_1x_n + p_2x_n^2 + \cdots + p_kx_n^k$ and $g = q_0 + q_1x_n + q_2x_n^2 + \cdots + q_lx_n^l$ where $k, l \in \mathbb{N}$ and $p_i, q_j \in \mathbb{F}[x_1, \ldots, x_{n-1}]$ for all $i = 0, 1, \ldots, k$ and $j = 0, 1, \ldots, l$. Use the assumption that $\mathbb{F}[x_1, \ldots, x_{n-1}]$ is an integral domain and a similar argument in the case $n = 1$, we can show that $f = g = 0$. This prove that $\mathbb{F}[x_1, \ldots, x_n]$ is also an integral domain.

Problem 3.6.10(Polynomial Functions).
Suppose $\mathbb{F}$ is an infinite field.

(1) Prove that polynomials $f, g \in \mathbb{F}[x]$ are equal if and only if $f(c) = g(c)$ for infinitely many $c \in \mathbb{F}$. Hence, f and g are equal if and only if they define the same polynomial function.

(2) More generally, use induction on n to show that $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ are equal if and only if $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ as functions.

Solution:

(1) If $f(x) = g(x) \in \mathbb{F}[x]$ are equal, then it is easy to see that $f(c) = g(c)$ for infinite many $c \in \mathbb{F}$ since $\mathbb{F}$ is an infinite field. Now assume there exist infinitely many $c \in \mathbb{F}$ such that $f(c) = g(c)$ for some $f, g \in \mathbb{F}[x]$. Note that by Exercise 3.6.9., for every $n \geq 1$, there exists different

$c_1, c_2, \dots, c_n \in \mathbb{F}$ such that

$$f(x) - g(x) = (x - c_1)(x - c_2) \cdots (x - c_n)q(x)$$

where $q(x) \in \mathbb{F}[x]$ is a polynomial. But $\deg(f-g)$ is finite, so it is only possible if $f(x) = g(x)$. Thus, we can conclude that f and g are equal if and only if they define the same polynomial function.

(2) We prove this by induction on the number n of indeterminates. When $n = 1$, this has been proved in (1). Now assume $n \geq 2$ and this is true for $\mathbb{F}[x_1, \dots, x_{n-1}]$.

Claim: If R is a commutative ring and an integral domain, then $c \in R$ is a root of $f \in R[x]$ if and only if f can be written as $f(x) = (x-c)q(x)$ where $q(x) \in R[x]$ and $\deg q(x) < \deg f(x)$.

Proof: Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$ for some $a_n, \dots, a_0 \in R$. There exists a polynomial $g(x) \in R[x]$ with leading term $a_n x^{n-1}$ such that

$$f(x) = (x - c)g(x) + r(x)$$

where $r(x) \in R[x]$ with $r(c) = 0$ and $\deg r(x) < \deg f(x)$. Repeat this process with $r(x)$ and finally we will obtain a polynomial of degree 1 which has c as its root, so it can only be $x - c$. This implies $x - c|f(x)$. ■

View $f, g \in \mathbb{F}[x_1, \dots, x_n]$ as polynomials in $R[x_n]$ with $R = \mathbb{F}[x_1, \dots, x_{n-1}]$. By our discussion in (1), $f = g$ if and only if $f(x_n) = g(x_n)$ as functions. This implies they have the same coefficents in R, by our assumption, $f = g$ if and only if $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$.

Problem 3.6.11

Suppose $\mathbb{F}$ is a finite field with $|\mathbb{F}| = q$. How many functions $f : \mathbb{F} \to \mathbb{F}$ are there? How many polynomials $f(x) \in \mathbb{F}[x]$ are there? Deduce that there are infinitely many different polynomials $f(x) \in \mathbb{F}[x]$ such that $f(c) = 0$ for all $c \in \mathbb{F}$. Give two examples of such polynomials.

Solution: $\mathbb{F}$ is a finite set with q elements. So there are q^2 functions $\mathbb{F} \to \mathbb{F}$. $\mathbb{F}[x]$ can be viewed as an infinite dimensional $\mathbb{F}$-vector space with basis $\{1, x, x^2, \dots, x^n, \dots\}$. By Exercise 1.6.5, we know that

$$|\mathbb{F}[x]| = \max(|\mathbb{F}|, \dim_{\mathbb{F}} \mathbb{F}[x]) = \aleph_0.$$

So the cardinality of polynomials over $\mathbb{F}$ is $\aleph_0$. Every polynomial can be viewed as a function $\mathbb{F} \to \mathbb{F}$, and since the number of functions is finite, we have infinite pairs of polynomials (f, g) with $f \neq g$ as polynomials in $\mathbb{F}[x]$ but $f(c) = g(c)$ for every $c \in \mathbb{F}$. Each pair (f, g) will give us a polynomial $f - g$ with $(f - g)(c) = 0$ for every $c \in \mathbb{F}$. For example, consider

$$\begin{aligned} h_1(x) &= (x - c_1)(x - c_2) \cdots (x - c_q), \\ h_2(x) &= (x - c_1)^2(x - c_2)^2 \cdots (x - c_q)^2 \end{aligned}$$

where $c_1, \dots, c_q$ are different elements in $\mathbb{F}$. It is easy to see that $h_1(x) \neq h_2(x)$ because $\deg h_1 = q \neq 2q = \deg h_2$, but for any $c \in \mathbb{F}$, we have $h_1(c) = h_2(c) = 0$.

Problem 3.7.19

Let X be a small set and $(X_i)_{i\in I}$ be the collection of all finite subsets of X. View I as a directed set so that $i \leq j \Leftrightarrow X_i \subset X_j$; then $(X_i)_{i\in I}$ is a direct system with $f_{i,j} : X_i \hookrightarrow X_j$ being the inclusion for all $i \leq j$. Show that $(X, (\iota_i)_{i\in I})$ is a direct limit of $(X_i)_{i\in I}$ in the category **Sets**, where $\iota_i : X_i \hookrightarrow X$ is the inclusion.

Solution: We prove this by showing that $(X, (\iota_i)_{i\in I})$ satisfies the universal property. Let Y be a set and for every $i \in I$, there exists a map $f_i : X_i \to H$ such that if $i \leq j$, we have a commutative diagram:

$$\begin{tikzcd}
X_i \arrow[rr, hook, "\text{inclusion}"] \arrow[dr, "f_i"'] & & X_j \arrow[dl, "f_j"] \\
& Y &
\end{tikzcd}$$

For every $x \in X$, consider all the one element set $\{x\} \subset X$. Since it is finite, we have $\{x\} \in (X_i)_{i\in I}$. So there exists a map $f_x : \{x\} \to Y$. Define $f : X \to Y$ by sending $x \in X$ to $f_x(x) \in Y$. This map is the unique map making the following diagram commutes:

$$\begin{tikzcd}
\{x\} \arrow[rr, "id"] \arrow[dr, hook] \arrow[ddr, "f_x"'] & & \{x\} \arrow[dl, hook'] \arrow[ddl, "f_x"] \\
& X & \\
& Y &
\end{tikzcd}$$

where $\{x\} \to X$ is the inclusion map. Moreover for any inclusion of finite set $X_i \hookrightarrow X_j$, we have a commutative diagram:

$$\begin{tikzcd}
X_i \arrow[rr, hook, "f_{i,j}"] \arrow[dr, hook, "\iota_i"] \arrow[ddr, "f_i"'] & & X_j \arrow[dl, hook', "\iota_j"'] \arrow[ddl, "f_j"] \\
& X \arrow[d, "f"] & \\
& Y &
\end{tikzcd}$$

The commutativity can be seen by the composition

$$\{x\} \hookrightarrow X_i \hookrightarrow X$$

for every $x \in X_i$ and for every $i \in I$. This proves that (X, ι_i) is the colimit of the direct system $(X_i)_{i\in I}$.

Problem 4.1.13

Let V be a two-dimensional vector space over $\mathbb{F}$ with basis x, y and set

$$t : 2x \otimes x \otimes x + x \otimes y \otimes y + y \otimes x \otimes y + y \otimes y \otimes x.$$

(1) For $\mathbb{F} = \mathbb{R}$ check that

$$t = (x + cy) \otimes (x + cy) \otimes (x + cy) + (x - cy) \otimes (x - cy) \otimes (x - cy)$$

where $c := 1/\sqrt{2}$. Deduce that t has rank 2.

(2) For $\mathbb{F} = \mathbb{Q}$ show that t has rank strictly greater than 2.

Solution:

(1) We have

$$\begin{aligned}
&(x + cy) \otimes (x + cy) \otimes (x + cy) \\
=&x \otimes x \otimes x + cx \otimes y \otimes x + cx \otimes x \otimes y + c^2 x \otimes y \otimes y \\
&+ cy \otimes x \otimes x + c^2 y \otimes y \otimes x + c^2 y \otimes x \otimes y + c^3 y \otimes y \otimes y
\end{aligned}$$

Note that $c = -\frac{1}{\sqrt{2}}$ is negative, so we have

$$\begin{aligned}
&(x + cy) \otimes (x + cy) \otimes (x + cy) + (x - cy) \otimes (x - cy) \otimes (x - cy) \\
=&2x \otimes x \otimes x + 2c^2 x \otimes y \otimes y + 2c^2 y \otimes y \otimes x + 2c^2 y \otimes x \otimes y \\
=&2x \otimes x \otimes x + x \otimes y \otimes y + y \otimes y \otimes x + y \otimes x \otimes y \\
=&t
\end{aligned}$$

We can see that t has rank 2.

(2) Assume the opposite. Suppose

$$t = f_1(x, y) \otimes f_2(x, y) \otimes f_3(x, y) + g_1(x, y) \otimes g_2(x, y) \otimes g_3(x, y)$$

where $f_i(x, y), g_i(x, y) \in \mathbb{Q}[x, y]$ for $i = 1, 2, 3$. If the degree of $f_i(x, y)$ is larger than 1, than the corresponding $g_i(x, y)$ must have the same leading term with opposite sign, so without loss of generality, we could assume every f_i and g_i are of degree 1 and have no constant terms. Write $f_i(x, y) = a_i x + b_i y$ and $g_i(x, y) = c_i x + d_i y$ where $a_i, b_i \in \mathbb{Q}$ for $i = 1, 2, 3$, we have

$$a_1 a_2 a_3 + c_1 c_2 c_3 = 2,$$

Problem 4.1.15

Assume that the ground field $\mathbb{F} = \mathbb{R}$. Show that

$$M_2(\mathbb{R}) \otimes M_2(\mathbb{R}) \cong M_4(\mathbb{R}) \cong \mathbb{H} \otimes \mathbb{H}$$

as $\mathbb{R}$-algebras.

Solution: Let $A, B \in M_2(\mathbb{R})$ be two 2×2 matrices where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. We define the following map

$$\begin{aligned} \phi : M_2(\mathbb{R}) \otimes M_2(\mathbb{R}) &\to M_4(\mathbb{R}), \\ A \otimes B &\mapsto \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix} \end{aligned}$$

To see that this is a well-defined map between $\mathbb{R}$-algebras, let $A_1, B_1, A_2, B_2 \in M_2(\mathbb{R})$. We have

$$\begin{aligned} &\phi((A_1 \otimes B_1)(A_2 \otimes B_2)) \\ =&\phi((A_1A_2) \otimes (B_1B_2)) \\ =&\phi(\begin{pmatrix} a_1a_2 + b_1c_2 & a_1c_2 + b_1d_2 \\ a_2c_1 + c_2d_1 & c_1c_2 + d_1d_2 \end{pmatrix} \otimes B_1B_2) \\ =&\begin{pmatrix} (a_1a_2 + b_1c_2)B_1B_2 & (a_1c_2 + b_1d_2)B_1B_2 \\ (a_2c_1 + c_2d_1)B_1B_2 & (c_1c_2 + d_1d_2)B_1B_2 \end{pmatrix} \\ =&\begin{pmatrix} a_1B_1 & b_1B_1 \\ c_1B_1 & d_1B_1 \end{pmatrix} \begin{pmatrix} a_2B_2 & b_2B_2 \\ c_2B_2 & d_2B_2 \end{pmatrix} \\ =&\phi(A_1 \otimes B_1)\phi(A_2 \otimes B_2) \end{aligned}$$

Moreover, ϕ is injective. Indeed, suppose $A \otimes B \in \ker \phi$. This means that

$$\begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

If $A = 0$, then $A \otimes B = 0 \otimes B = 0$. If there is at least one nonzero entry in A, for example $a \neq 0$, then $aB = 0$ being the zero matrix implies that $B = 0$, and we have $A \otimes B = A \otimes 0 = 0$. Note that

$$\dim(M_2(\mathbb{R}) \otimes M_2(\mathbb{R})) = (\dim(M_2(\mathbb{R})))^2 = 16 = \dim M_4(\mathbb{R}).$$

So ϕ is an isomorphism.

Recall that the quaternions $\mathbb{H}$ over $\mathbb{R}$ has a basis $\{1, i, j, k\}$ with multiplication $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. View $\mathbb{H}$ as a 4-dimensional $\mathbb{R}$-vector space. And we know that $End_{\mathbb{R}}(\mathbb{H}) \cong M_4(\mathbb{R})$. Define a bilinear map

$$\begin{aligned} \mathbb{H} \times \mathbb{H} &\to End_{\mathbb{R}}(\mathbb{H}), \\ (a, b) &\mapsto (h \mapsto ah\bar{b}). \end{aligned}$$

where

$$\bar{b} = \overline{b_1 + b_2 i + b_3 j + b_4 k} = b_1 - b_2 i - b_3 j - b_4 k.$$

This map induces a linear map $\psi : \mathbb{H} \otimes \mathbb{H} \to End_{\mathbb{R}}(\mathbb{H})$. Let $(a, b) \in \ker \psi$. For every $h \in H$, we have $ah\bar{b} = 0$. Note that $\mathbb{R}$ has characteristic 2, so either a or $\bar{b}$ must 0. Thus, $a \otimes b = 0$ and ψ is injective. Moreover, we know that

$$\dim(\mathbb{H} \otimes \mathbb{H}) = 16 = \dim(End_{\mathbb{R}}(\mathbb{H})).$$

So we have the isomorphisms

$$\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R}) \cong M_2(\mathbb{R}) \otimes M_2(\mathbb{R}).$$

Problem 4.2.12(Duaility of symmetric and divided powers).
Let V be a finite dimensional vector space. From Example 4.1.3, we get a natural isomorphism $T^n(V^*) \xrightarrow{\sim} T^n(V)^*$ mapping a pure tensor $f_1 \otimes \cdots \otimes f_n \in T^n(V^*)$ to the unique linear map $f_1 \bar{\otimes} \cdots \bar{\otimes} f_n : T^n(V) \to \mathbb{F}$ which sends $v_1 \otimes \cdots \otimes v_n \in T^n(V)$ to $f(v_1) \cdots f(v_n)$. Composing the dual map π^* to the quotient map $\pi : T^n(V) \to S^n(V)$ with this isomorphism gives a linear map $\pi^* : S^n(V)^* \hookrightarrow T^n(V^*)$. Prove that π^* is an isomorphism between $S^n(v)^*$ and $\Gamma^n(V^*)$.

Solution:

Problem 4.3.17
Let V be a vector space.

(1) Vectors $v_1, \ldots, v_m \in V$ are linearly independent if and only if $v_1 \wedge \cdots \wedge v_m \neq 0$ in $\bigwedge^m V$.

(2) Let $v_1, \ldots, v_m$ and $w_1, \ldots, w_m$ be two linearly independent systems of vectors in V. Show that $\mathbb{F}v_1 + \cdots + \mathbb{F}v_m = \mathbb{F}w_1 + \cdots + \mathbb{F}w_m$ if and only if $v_1 \wedge \cdots \wedge v_m$ is proportional to $w_1 \wedge \cdots \wedge w_m$ in $\bigwedge^m V$.

(3) Show that there is a well-defined embedding $Gr_m(V) \hookrightarrow \mathbb{P}(\bigwedge^m V)$ sending a subspace with basis $v_1, \ldots, v_m$ to the line spanned by $v_1 \wedge \cdots \wedge v_m$.

(4) Give an example to show that the map from (3) is not surjective in general.

Solution:

Problem 4.4.4
Assume $\mathrm{char}\mathbb{F} = 2$. Then a *quadratic form* on a vector space V is a function $Q : V \to \mathbb{F}$ such that $Q(\lambda v) = \lambda^2 Q(v)$ and $Q(v + w) = Q(v) + Q(w) + (v|w)$ for some (necessarily unique) bilinear form $(-|-) : V \times V \to \mathbb{F}$. Show that the form $(-|-)$ is skew-symmetric. Convince yourself that you cannot recover Q from $(-|-)$.

Solution: Because char$\mathbb{F} = 2$, for any $v \in V$, we have

$$(v|v) = Q(v+v) + Q(v) + Q(v) = Q(2v) + 2Q(v) = 0.$$

Thus, $(-|-)$ is skew-symmetric. Q cannot be recovered from $(-|-)$ since 2 is not invertible in $\mathbb{F}$.

Problem 4.4.9
Let V be a finite dimensional vector space equipped with a non-degenerate skew-symmetric bilinear form $(-|-)$. If $V \subseteq V$ is an isotropic subspace with basis $u_1, \ldots, u_m$, then there exists an isotropic subspace U', with basis $u'_1, \ldots, u'_m$ such that $U \cap U' = 0$ and $(u_i|u'_j) = \delta_{i,j}$ for all $1 \leq i, j \leq m$.

Solution:

Problem 4.4.10(Witt's Theorem for skew-symmetric bilinear form).
Let V be a finite dimensional vector space equipped with a non-degenerate skew-symmetric bilinear form. Let U be a subspace of V with the induced bilinear form. Prove that any isometric embedding $f : U \hookrightarrow V$ of U into V can be extended to an isometry $\hat{f} : V \to V$.

Solution:

Problem 4.4.12(Pfaffians).
Assume that $\mathbb{F}$ is of characteristic zero. Let $n = 2m$ be even and $A = [a_{ij}]_{1 \leq i,j \leq n}$ be an $n \times n$ skew-symmetric matrix with entries in $\mathbb{F}$. Let V be a vector space with basis $v_1, \ldots, v_n$ and set $a := \sum_{1 \leq i,j \leq n} a_{ij} v_i \wedge v_j \in \bigwedge^2(V)$.

(1) Prove that $a^m = 2^m m! (\operatorname{Pf} A) v_1 \wedge \cdots \wedge v_n$ (mth power taken in the exterior algebra $\wedge(V)$.

(2) For any matrix $P = [p_{ij}]_{1 \leq i,j \leq n}$, show that $\operatorname{Pf}(P^T A P) = (\det P)(\operatorname{Pf} A)$.

(3) Show that $\det A = (\operatorname{Pf} A)^2$.

Solution:

Problem 6.1.12
Let H be a characteristic subgroup of G. Prove:

(1) If G is a characteristic subgroup of K, then H is a characteristic subgroup of K.

(2) If $G \trianglelefteq K$, then $H \trianglelefteq K$.

(3) If K is a characteristic subgroup of G, then HK and $H \cap K$ are characteristic subgroups of G.

Solution:

(1) Let $\phi : K \to K$ be a group automorphism. We know that $\phi(G) \subset G$ since G is a characteristic subgroup of K. This means that ϕ can be viewes as a group automorphism of G. Thus, $\phi(H) \subset H$ because H is a characteristic subgroup of G. This proves that H is a characteristic subgroup of K.

(2) For any $k \in K$, we have $kHk^{-1} \subset G$ since G is a normal subgroup of K. Note that in this case we have a group automorphism:

$$\begin{aligned} \phi : G &\to G, \\ g &\mapsto kgk^{-1}. \end{aligned}$$

And because H is a characteristic subgroup of G, we have $\phi(H) \subset H$. This proves that $kHk^{-1} = H$. H is a normal subgroup of K.

(3) For any $hk \in HK$ and any automorphism $\phi : G \to G$, we have $\phi(gh) = \phi(g)\phi(h) \in HK$ since both H and K are characteristic subgroups of G. Similarly for any $a \in H \cap K$, we have $\phi(a) \in H \cap K$. So HK and $H \cap K$ are characteristic subgroups of G.

Problem 6.2.17

Let p be a prime.

(1) Construct an isomorphism between C_{p^∞} and the subgroup of $\mathbb{C}^\times$ which consists of all p^nth roots of 1 for all $n \in \mathbb{Z}_{\geq 0}$.

(2) Explain why the map $g \mapsto g^p$ yields an isomorphism $C_{p^\infty}/C_p \cong C_{p^\infty}$.

(3) C_{p^∞} is not finitely generated.

(4) Describe all subgroups of C_{p^∞}.

(5) Any non-trivial quotient of C_{p^∞} is isomorphic to C_{p^∞}.

Solution:

Problem 6.2.18

Let p be a prime and $\mathbb{Q}_{(p)}$ be a subgroup of $(\mathbb{Q}, +)$ which consists of all numbers of the form m/p^n for $m, n \in \mathbb{Z}$.Use the map

$$\begin{aligned} \mathbb{Q}_{(p)} &\to C_{p^\infty}, \\ m/p^n &\mapsto e^{2\pi i m/p^n} \end{aligned}$$

to deduce an isomorphism $\mathbb{Q}_{(p)}/\mathbb{Z} \cong C_{p^\infty}$.

Solution:

Problem 6.3.8
Let p be a prime, σ be any p-cycle in S_p and τ be any transposition in S_p. Prove that $\langle \sigma, \tau \rangle = S_p$.

Solution:

Problem 6.5.3(Elements of $O(2)$).

(a) The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is orthogonal if and only if $a^2 + c^2 = b^2 + d^2 = 1$ and $ab + cd = 0$.

(b) Deduce that a matrix if orthogonal if and only if it looks like

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \tag{1}$$

or

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \tag{2}$$

for some $\alpha \in \mathbb{R}$.

(c) Prove that a matrix is in $SO(2)$ if and only if it is of the form (1) for some $\alpha \in \mathbb{R}$.

(d) The linear transformation whose matrix is of the form (1) is the rotation through the angle α; the linear transformation whose matrix is of the form (2) is the reflection through the line forming the angle $\alpha/2$ with the x-axis.

(e) The group $O(2)$ is generated by reflections.

Solution:

(a) A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is orthogonal if and only if $A^T A = I_2$, written as

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This is the same as the following equations:

$$\begin{aligned} a^2 + c^2 &= 1, \\ ab + cd &= 0, \\ b^2 + d^2 &= 1. \end{aligned}$$

(b) It is easy to check directly that this is a sufficient condition. We prove that it is also necessary. Since $a^2 + c^2 = 1$, we know there exists some $\alpha \in \mathbb{R}$ such that $a = \cos\alpha$ and $c = \sin\alpha$. If

$a = \cos\alpha = 0$, then $c^2 = \sin^2\alpha = 1$, and $ab + cd = 0$ tells us that $d = 0$. Thus, $b^2 = 1$. Since $b^2 = d^2 = 1$, if $b = d$ then A has the form (2). If $b = -d$, then A has the form (1). Now suppose $a = \cos\alpha \neq 0$. We can write

$$b = -\frac{d\sin\alpha}{\cos\alpha}.$$

Plug this into $b^2 + d^2 = 1$, and we have

$$d^2(1 + \frac{\sin^2\alpha}{\cos^2\alpha}) = \frac{d^2}{\cos^2\alpha} = 1.$$

If $d = \cos\alpha$, then A has the form (1). If $d = -\cos\alpha$, then A has the form (2).

(c) A matrix A is in $SO(2)$ if and only if A is orthogonal and $\det A = 1$. From what we have proved in (b), A must be of the form (1).

(d) Given a point nonzero point $v = (x, y) \in \mathbb{R}^2$ and a matrix A of the form (1). The linear transformation associated with A maps v to

$$Av = (x\cos\alpha - y\sin\alpha, x\sin\alpha + y\cos\alpha).$$

We can see that

$$|Av|^2 = (x\cos\alpha - y\sin\alpha)^2 + (x\sin\alpha + y\cos\alpha)^2 = x^2 + y^2 = |v|^2.$$

And moreover, the angle θ between the vector v and Av can be calculated as

$$\cos\theta = \frac{v \cdot Av}{|v||Av|} = \frac{(x^2 + y^2)\cos\alpha}{x^2 + y^2} = \cos\alpha.$$

So A is the rotation through angle α.

Now assume the linear transformation has the form (2). In this case, Av can be written as

$$Av = (x\cos\alpha + y\sin\alpha, x\sin\alpha - y\cos\alpha).$$

We still have $|Av|^2 = x^2 + y^2 = |v|^2$ and consider the line represented by the vector $w = (\cos\frac{\alpha}{2}, \sin\frac{\alpha}{2})$. The angle θ_1 between v and w is

$$\cos\theta_1 = \frac{v \cdot w}{|v|} = \frac{x\cos\frac{\alpha}{2} + y\sin\frac{\alpha}{2}}{x^2 + y^2}.$$

and the angle θ_2 between Av and w is

$$\cos\theta_2 = \frac{Av \cdot w}{|Av|} = \frac{x(\cos\alpha\cos\frac{\alpha}{2} + \sin\alpha\sin\frac{\alpha}{2}) + y(\sin\alpha\cos\frac{\alpha}{2} - \cos\alpha\sin\frac{\alpha}{2})}{x^2 + y^2} = \frac{x\cos\frac{\alpha}{2} + y\sin\frac{\alpha}{2}}{x^2 + y^2}.$$

This shows that $\theta_1 = \theta_2$ and we can conclude that A of the form (2) is the reflection through the line forming the angle $\frac{\alpha}{2}$ with the x-axis.

(e) We prove that the matrices of the form (1) can be generated by the matrices of the form

(2), namely reflections. Write $A = R(\alpha)$ is of the form (1) (rotation) for some $\alpha \in \mathbb{R}$ and $A = F(\beta)$ is of the form (2) (reflection) for some $\beta \in \mathbb{R}$.

Claim: For any $\alpha \in \mathbb{R}$, we have $R(\alpha) = F(\pi)F(\pi - \alpha)$.

Proof: Just some computation.

$$\begin{aligned} F(\pi)F(\pi-\alpha) &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos(\pi-\alpha) & \sin(\pi-\alpha) \\ \sin(\pi-\alpha) & -\cos(\pi-\alpha) \end{pmatrix} \\ &= \begin{pmatrix} -\cos(\pi-\alpha) & -\sin(\pi-\alpha) \\ \sin(\pi-\alpha) & -\cos(\pi-\alpha) \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \\ &= R(\alpha). \end{aligned}$$

■

The claim above shows that an orthogonal matrix can be written as a product of reflections, thus $O(2)$ is generated by reflections.

Problem 6.5.5

Let $c_1, \dots, c_l \in \mathbb{F}$ satisfy $c_1 + \cdots + c_l = 1$, and $v_1, \dots, v_l \in V$. If f is an affine transformation of V, then

$$f(c_1v_1 + \cdots + c_lv_l) = c_1f(v_1) + \cdots + c_lf(v_l).$$

Deduce that f fixes points $v \neq w$ in V only if it fixes every point of the line through v and w.

Solution: We know that $AGL(V) = GL(V)T(V)$, so an affine transformation f can be written as $f = gt_w$ where $g \in GL(V)$ is a linear transformation and t_w is a translation. Now we have

$$\begin{aligned} f(c_1v_1 + \cdots + c_lv_l) &= gt_w(c_1v_1 + \cdots + c_lv_l) \\ &= g(c_1v_1 + \cdots + c_lv_l + w) \\ &= c_1g(v_1) + \cdots + c_lg(v_l) + g(w) \\ &= c_1g(v_1) + \cdots + c_lg(v_l) + (c_1 + \cdots + c_l)g(w) \\ &= c_1(g(v_1) + g(w)) + \cdots + c_l(g(v_l) + g(w)) \\ &= c_1(gt_w)(v_1) + \cdots + c_l(gt_w)(v_l) \\ &= c_1f(v_1) + \cdots + c_lf(v_l). \end{aligned}$$

Now suppose f fixes points $v, w \in V$ with $v \neq w$. Any point on the line through v and w can be written as $c_1v + c_2w$ for some $c_1, c_2 \in \mathbb{F}$ satisfying $c_1 + c_2 = 1$. So by the previous discussion, we have

$$\begin{aligned} f(c_1v + c_2w) &= c_1f(v) + c_2f(w) \\ &= c_1v + c_2w. \end{aligned}$$

We can see that $c_1v + c_2w$ is also a fixed point of f.

Problem 6.5.6

Suppose that the ground field $\mathbb{F}$ has characteristic 0. If G is a finite subgroup of $AGL(V)$ then there is an element $v \in V$ fixed by every element of G.

Solution:

Problem 6.5.8

(1) The group $AO(2)$ of motions of the Euclidean space $\mathbb{R}^2$ is generated by reflections relative to arbitrary lines.

(2) Each element of the group $ASO(2)$ of rigid motions of $\mathbb{R}^2$ is either a tranlation or a rotation about some point.

Solution:

Problem 6.6.4(Finite subgroups of $O(2)$).

Let G be a finite subgroup of $O(2)$. Then G is one of the following:

(i) $G = C_n$, the cyclic group of order n generated by the rotation through $2\pi/n$;

(ii) $G = D_{2n}$, the dihedral group of order $2n$ generated by the rotation through $2\pi/n$ and a reflection about a line through the origin.

Solution:

Problem 6.6.6(Symmetries of a cube)

Let C^3 be a regular cube in $\mathbb{R}^3$. Use the action of $\mathrm{Sym}_+(C^3)$ on the four diagonals of the cube to show that $\mathrm{Sym}_+(C^3) \cong S_4$. Show that $\mathrm{Sym}(C^3) \cong S_4 \times C_2$. Any idea on $\mathrm{Sym}_+(C^n)$ and $\mathrm{Sym}(C^n)$?

Solution:

Problem 6.7.5

Prove that the group of upper unitriangular 3×3 matrices over $\mathbb{F}_3$ is non-abelian and has exponent 3.

Solution: Let $A = \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & d & f \\ & 1 & e \\ & & 1 \end{pmatrix}$ where $a, b, c, d, e, f \in \mathbb{F}_3$. We have

$$AB = \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & d & f \\ & 1 & e \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & c+f+ae \\ & 1 & b+e \\ & & 1 \end{pmatrix}.$$

On the other hand, we have

$$BA = \begin{pmatrix} 1 & a+d & c+f+bd \\ & 1 & b+e \\ & & 1 \end{pmatrix}.$$

So $AB \neq BA$ unless $bd = ae$. For example,

$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 2 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 2 \\ & & 1 \end{pmatrix}.$$

For any upper unitriangular matrix $A = \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix}$, we have

$$A^3 = \begin{pmatrix} 1 & 3a & 3ab+3c \\ & 1 & 3b \\ & & 1 \end{pmatrix} = I_3 \in GL_3(\mathbb{F}_3).$$

So this group has exponent 3.

Problem 6.7.6

Let G be a finitely generated group. Assume that $g^3 = 1$ for all $g \in G$.

(a) Show that G is finite.

(b) Assume further that G is generated by two elements. Show that $|G| \leq 27$ and that this estimate cannot be improved.

Solution:

Problem 6.8.7

The group of upper unitriangular 3×3 matrices over $\mathbb{F}_3$ from Exercise 6.7.5. is of the form $C_3 \ltimes (C_3 \times C_3)$.

Solution: Denote by G the group of 3×3 upper unitriangular matrices over $\mathbb{F}_3$. Consider the following group homomorphism

$$\begin{aligned} C_3 &\to G, \\ a &\mapsto \begin{pmatrix} 1 & a & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} C_3 \times C_3 &\to G, \\ (b,c) &\mapsto \begin{pmatrix} 1 & 0 & c \\ & 1 & b \\ & & 1 \end{pmatrix}. \end{aligned}$$

These are well-defined group homomorphisms. Consider the group homomorphism

$$\begin{aligned} \phi : C_3 &\to \mathrm{Aut}(C_3 \times C_3), \\ a &\mapsto (\phi(a) : (b,c) \to (b, ab + c)). \end{aligned}$$

The multiplication in the semidirect product $C_3 \ltimes (C_3 \times C_3)$ is given by

$$(a,b,c) \cdot (d,e,f) = (a+d, b+\phi(a)(e), c+\phi(a)(f)) = (a+d, b+e, c+f+ae)$$

which is exactly the matrices multiplication

$$\begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & d & f \\ & 1 & e \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & c+f+ae \\ & 1 & b+e \\ & & 1 \end{pmatrix}.$$

Note that $a,b,c,d,e,f \in \mathbb{F_3} \cong C_3$. We have an isomorphism $G \cong C_3 \ltimes (C_3 \times C_3)$.
