1.9.1

Claim: $\forall n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Proof: Base case: When $n = 1$, $(x+y)^1 = x + y$ is obviously true. Hypothesis: When $n = m$,

$$(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k$$

is true.

Then when $k = m + 1$,

$$\begin{aligned}
(x+y)^{m+1} &= (x+y)^m \cdot (x+y) \\
&= (\sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k) \cdot (x+y) \\
&= x \cdot \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k + y \cdot \sum_{j=0}^{m} \binom{m}{j} x^{m-j} y^j \\
&= \sum_{k=0}^{m} \binom{m}{k} x^{m+1-k} y^k + \sum_{j=0}^{m} \binom{m}{j} x^{m-j} y^{j+1} \\
&= \sum_{k=0}^{m} \binom{m}{k} x^{m+1-k} y^k + \sum_{j=0}^{m} \binom{m}{j+1-1} x^{m+1-j-1} y^{j+1} \\
&= \sum_{k=0}^{m} \binom{m}{k} x^{m+1-k} y^k + \sum_{k=1}^{m} \binom{m}{k-1} x^{m+1-k} y^k \\
&= \sum_{k=0}^{m+1} \binom{m}{k} x^{m+1-k} y^k - \binom{m}{m-1} x^0 y^k + \sum_{k=0}^{m+1} \binom{m}{k-1} x^{m+1-k} y^k - \binom{m}{-1} x^{m+1} y^0 \\
&= \sum_{k=0}^{m+1} [\binom{m}{k} + \binom{m}{k-1}] x^{m+1-k} y^k \\
&= \sum_{k=0}^{m+1} \binom{m+1}{k} x^{m+1-k} y^k
\end{aligned}$$

Thus, we can conclude that $\forall n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \blacksquare$$

1.10.2

Claim: $C_4 = \{i, -1, -i, 1\}$ is a group under complex multiplication.

	i	-1	$-i$	1
i	-1	$-i$	1	i
-1	$-i$	1	i	-1
$-i$	1	i	-1	$-i$
1	i	-1	$-i$	1

Table 1: Table of Multiplication of C_4

Proof: As the table above has shown, the set under complex multiplication has an identity 1, and the inverses:

- $(i)^{-1} = -i$
- $(-1)^{-1} = -1$
- $(-i)^{-1} = i$
- $(1)^{-1} = 1$

And the closure is fulfilled and associativity is guaranteed by the associativity of $\mathbb{C}$.

As a result, we can conclude that $C_4 = \{i, -1, -i, 1\}$ is a group under complex multiplication. $\blacksquare$

1.10.4

Claim: There exists at least 1 isomorphism between C_4 and $\mathbb{Z}_4$.

Proof: It is easy to construct the following the bijections $f : C_4 \mapsto \mathbb{Z}_4$:

- $f(i) = [1]$
- $f(-1) = [2]$
- $f(-i) = [3]$
- $f(1) = [0]$

that make the multiplication tables match up.

So it is true that there exists at least 1 isomorphism between C_4 and $\mathbb{Z}_4$ $\blacksquare$.

1.10.9

Claim: Affine transformations Aff $= \{f | f : \mathbf{x} \mapsto S(\mathbf{x}) + \mathbf{b}\}$ forms a group under composition of maps.

Proof:

- Closure:
  Let $f = S_1(\mathbf{x}) + \mathbf{b}_1$ and $g = S_2(\mathbf{x}) + \mathbf{b}_2 \in$ Aff, then $f \circ g = S_1(S_2(\mathbf{x}) + \mathbf{b}_2) + \mathbf{b}_1 = S_1(S_2(\mathbf{x}) + \mathbf{b}_2) + \mathbf{b}_1 = S_1(S_2(\mathbf{x})) + S_1(\mathbf{b}_2) + \mathbf{b}_1 \in Aff$ which means any transformation composition form of arbitrary 2 affine transformations.

- Associativity:
  Let $f = S_1(\mathbf{x}) + \mathbf{b}_1$, $g = S_2(\mathbf{x}) + \mathbf{b}_2$, $h = S_3(\mathbf{x}) + \mathbf{b}_3 \in T$.

  Then $f \circ g \circ h = (S_1(S_2(\mathbf{x}) + \mathbf{b}_2) + \mathbf{b}_1) \circ (S_3(\mathbf{x}) + \mathbf{b}_3) = S_1(S_2(S_3(\mathbf{x}) + \mathbf{b}_3) + \mathbf{b}_2) + \mathbf{b}_1 = S_1(S_2(S_3(\mathbf{x}))) + S_1(S_2(\mathbf{b}_3)) + S_1(\mathbf{b}_2) + \mathbf{b}_1$.

  $f \circ (g \circ h) = (S_1(\mathbf{x}) + \mathbf{b}_1) \circ (S_2(S_3(\mathbf{x}) + \mathbf{b}_3) + \mathbf{b}_2) = (S_1(\mathbf{x}) + \mathbf{b}_1) \circ (S_2(S_3(\mathbf{x})) + S_2(\mathbf{b}_3) + \mathbf{b}_2) = S_1(S_2(S_3(\mathbf{x}))) + S_1(S_2(\mathbf{b}_3)) + S_1(\mathbf{b}_2) + \mathbf{b}_1$.

  Thus, $f \circ g \circ h = f \circ (g \circ h)$, which means its associativity is proved.

- Identity:
  It's obvious that $f(\mathbf{x}) = \mathbf{x}$ satisfy that $f \circ g = g$.

- Inverse:
  The inverse of affine transformation f^{-1} satisfy $f \circ f^{-1} = f^{-1} \circ = e$, so for $f(x) = S_1(x) + \mathbf{b}_1, f^{-1}(\mathbf{x}) = S_2(\mathbf{x}) + \mathbf{b}_2$, $f \circ f^{-1} = f^{-1} \circ = S_1(S_2(\mathbf{x})) + S_1(\mathbf{b}_2) + \mathbf{b}_1$. To make this equal to identity, we need

$S_1(S_2(\mathbf{x})) = x$, and $S_1(\mathbf{b}_2) + \mathbf{b}_1 = 0$. Since S_1, S_2 are all invertible transformation, so the first condition can always be satisfied. And since the set of all n-dimension vectors form a group under addition, the second condition can be satisfied as well. Thus, for any affine transformation f, we can always find its inverse.

As a result, we can conclude that affine transformations $\text{Aff} = \{f | f : \mathbf{x} \mapsto S(\mathbf{x}) + \mathbf{b}\}$ forms a group under composition of maps $\blacksquare$.

1.11.2

Claim: Let K be any field, set $K[x]$ of polynomials with coefficients in K form a commutative ring under usual addition and multiplication of polynomials. And the constant polynomial 1 is the multiplicative identity, and the only units are the constant polynomials.

Proof: Prove it's a commutative ring first:
And to prove that this set is a commutative ring, we need to prove its an abelian group under addition first.
Let f, g, h be 2 arbitrary polynomials with coefficient in field K.
Since K is a field, so we know that $\forall f \in K[x], x \in K, f(K) \in K$

Closure: Thus, the addition

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{n_2} (e_{1i} + e_{2i}) x^i + \sum_{i=n_2+1}^{n_1} e_{1i} x^i$$

which is in $K[x]$, so the closure is proved.

Associativity: Then

$$\begin{aligned}
((f+g)+h)(x) &= (f(x)+g(x)) + h(x) \\
&= \sum_{i=0}^{n_2} (e_{1i} + e_{2i}) x^i + \sum_{i=n_2+1}^{n_1} (e_{1i} + e_{2i}) x^i + \sum_{i=0}^{n_3} e_{3i} x^i \\
&= \sum_{i=0}^{n_2} (e_{1i} + e_{2i} + e_{3i}) x^i + \sum_{i=n_2+1}^{n_1} (e_{1i} + e_{2i}) x^i + \sum_{i=0}^{n_3} e_{3i} x^i
\end{aligned}$$

$$\begin{aligned}(f+(g+h)(x)) &= f(x)+(g(x)+h(x))\\ &= \sum_{i=0}^{n_2} e_{1i}x^i + \sum_{i=0}^{n_3}(e_{2i}+e_{3i})x^i + \sum_{i=n_3+1}^{n_2} e_{3i}\\ &= \sum_{i=0}^{n_2}(e_{1i}+e_{2i}+e_{3i})x^i + \sum_{i=n_2+1}^{n_1}(e_{1i}+e_{2i})x^i + \sum_{i=0}^{n_3} e_{3i}x^i\end{aligned}$$

which means that $((f+g)+h)(x) = (f+(g+h)(x))$. So the associativity is proved.

Commutativity:

$$f+g = \sum_{i=0}^{n_2}(e_{1i}+e_{2i})x^i + \sum_{i=n_2+1}^{n_1} e_{1i}x^i = g+f$$

which means the commutativity is proved to be true.

Identity: $f(x)=0$ fulfills the requirement that $0+f=f+0=f$. So the identity is $f(x)=0$.

Inverse: For an arbitrary polynomial f, we want to find a $f^{-1}=-f$ that $f+(-f)=0$.

As a result, we can conclude that $K[x]$ is an abelian group.

Then we can start working on proving that $k[x]$ forms a commutative monoid under the multiplication.

Closure:

$$\begin{aligned}f\cdot g &= (\sum_{i=0}^{n_1} e_{1i}x^i)(\sum_{i=0}^{n_2} e_{2i}x^i)\\ &= (e_{10}x^0 + e_{11}x^1 \cdots + e_{1n_1}^{n_1})\sum_{i=0}^{n_2} e_{2i}x^i\\ &= \sum_{i=0}^{n_2}(e_{10}x^0 + e_{11}x^1 \cdots + e_{1n_1}^{n_1})e_{2i}x^i\end{aligned}$$

Since $f(x) \in K$, we denote it as e', then

$$f \cdot g = \sum_{i=0}^{n_2} (e' e_{2i}) x^i \in K[x]$$

Thus, the closure under multiplication is proved.

Associativity

$$\begin{aligned}
(f \cdot g) \cdot h &= (\sum_{j=0}^{n_2}((\sum_{i=0}^{n_1} e_{1i}x^j)e_{2j})x^j) \cdot (\sum_{k=0}^{n_3} e_{3j}x^k) \\
&= \sum_{k=0}^{n_3}(\sum_{j=0}^{n_2}((\sum_{i=0}^{n_1} e_{1i}x^i)e_{2j})x^j)e_{3k})x^k
\end{aligned}$$

$$\begin{aligned}
f \cdot (g \cdot h) &= (\sum_{i=0}^{n_1} e_{1i}x^i) \cdot (\sum_{k=0}^{n_3}((\sum_{j=0}^{n_2} e_{2j}x^j)e_{2k})x^k) \\
&= \sum_{k=0}^{n_3}((\sum_{i=0}^{n_1} e_{1i}x^i)((\sum_{j=0}^{n_2} e_{2j}x^j)e_{2k}))x^k \\
&= \sum_{k=0}^{n_3}(\sum_{j=0}^{n_2}((\sum_{i=0}^{n_1} e_{1i}x^i)e_{2j})x^j)e_{3k})x^k
\end{aligned}$$

Thus, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$, and multiplication of $k[n]$ is associative.

Identity: Since for all f, we have $f \cdot 1 = 1 \cdot f = f$, its the identity of multiplication of $K[x]$

Commutativity:

$$f \cdot g = \sum_{j=0}^{n_2}((\sum_{i=0}^{n_1} e_{1i}x^j)e_{2j})x^j = g \cdot f$$

Thus, the requirement of commutativity is fulfilled.

Finally, we can work on the distributability of $+$ and $\cdot$ operations.

$$
\begin{aligned}
f(g+h) &= (\sum_{i=0}^{n_1} e_{1i}x^i)(\sum_{j=0}^{n_3}(e_{2j}+e_{3j})x^j) \\
&= (\sum_{i=0}^{n_1} e_{1i}x^i)(\sum_{j=0}^{n_3} e_{2j} + \sum_{j=0}^{n_3} e_{3j}x^j) \\
&= (\sum_{i=0}^{n_1} e_{1i}x^i)(\sum_{j=0}^{n_3} e_{2j}) + (\sum_{i=0}^{n_1} e_{1i}x^i)(\sum_{j=0}^{n_3} e_{3j}x^j) \\
&= fg + fh
\end{aligned}
$$

Similarly, $(f+g)h = fh + gh$, so the distributability is proved.

And by definition, a unit is an element with a multiplicative inverse. Which is saying that for a unit f, there is a $f-1$ that $f \cdot f^{-1} = 1$. Since product of any 2 non-zero $x \in K$ will not be zero, the terms generated by the products of non-zero degree terms of 2 polynomials will not be cancelled out. As a result, only 0-degree polynomials, namely, constant polynomials are the only units.

In conclusion, $K[x]$ of polynomials with coefficients in K form a commutative ring under usual addition and multiplication of polynomials. And the constant polynomial 1 is the multiplicative identity and constant polynomials are the only units.$\blacksquare$