Chapter 21

C5.

for \( n = 1 \), \( 1 = \frac{1}{6}(1+1)(2+1) \).

Assume for any \( k \in \mathbb{N} \),
\[
1^2 + 2^2 + \ldots + k^2 = \frac{1}{6}k(k+1)(2k+1).
\]

\[
\begin{align*}
1^2 + 2^2 + \ldots + (k+1)^2 &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\
&= \frac{1}{6}(k+1) \left[ 2k^2 + k + 6k + 6 \right] \\
&= \frac{1}{6}(k+1) \left[ 2k^2 + 7k + 6 \right] \\
&= \frac{1}{6}(k+1)(k+2)(k+3) = \frac{1}{6}(k+1)(k+1+1)(2(k+1)+1)
\end{align*}
\]

H2. Show \( \forall n \in \mathbb{N} \), \( n \in K \).

By induction.

\( \forall n \geq 1 \), assume \( \forall k < n \), \( k \in K \).

by (ii) \( n \in K \).

H2. Show \( (S, \leq, \forall n \in \mathbb{N}, (\forall k < n, S_k) \Rightarrow (S_k)) \Rightarrow (\forall n \in \mathbb{N}, S_n) \).

Assume \( S_k \) & \( \forall n \in \mathbb{N} \), \( \forall k < n \), \( S_k \).

Assume \( \neg S_n \), for some \( n \in \mathbb{N} \).

Define \( S = \{ n \in \mathbb{N} \mid \neg S_n \} \) is not empty.

\( \mathbb{N} \) is well-ordering, there exists the least \( s \in S \).

Since \( S_k \), \( s + 1 \), \( s \geq 2 \), \( \forall k < s \), \( S_k \). Since \( s \) is the least but by assumption \( S_k \), \( s \leq s \).

Note: by \( S_k \), I mean \( S_k \) is true. \( \neg S_k \) means \( S_k \) is false.

Chapter 22.

C2. Since \( (a, c) = 1 \), \( ma + nc = 1 \) for some \( m, n \in \mathbb{Z} \).

\[
\begin{align*}
macb + ncb &= b \\
|ab|, \ c|cb|, \ c|mab + ncb &= b
\end{align*}
\]

F6. Show: \( \text{lcm}(a, b) = ab \).

It suffice to show: for any \( x \in \mathbb{N} \), \( (a|bx, b|lx) \Rightarrow (ab|lx) \).

Let \( x \in \mathbb{N} \) be s.t \( a|bx, b|lx \).

\( b|x \) \( \Rightarrow x = mb \) for some \( m \in \mathbb{Z} \), \( a|x \) \( \Rightarrow a|m \).

\( m = an \) for some \( n \in \mathbb{Z} \). \( \Rightarrow x = mb = anb \). \( \Rightarrow ab|x \).
C3. Let \( p \) be a prime number.

Show: \( \mathbb{Z}_p \) is a field.

\( (\mathbb{Z}_p, +) \) is an abelian group.

It suffices to show \( (\mathbb{Z}_p \setminus \{0\}, \cdot) \) is abelian group.

It suffices to show that for any \( x \in \mathbb{Z}_p \setminus \{0\} \), there exist \( y \in \mathbb{Z}_p \setminus \{0\} \) s.t. \( xy = 1 \).

For any \( x \in \mathbb{Z}_p \setminus \{0\} \), \( x = [n] \) for some new \( n \) s.t. \( n < p \).

\( (n, p) = 1 \), \( xn + yp = 1 \) for some \( x, y \in \mathbb{Z} \).

\( \{xn + yp\} = 1 \)

\( \{x[n] + [y]p\} = 1 \) \( \Rightarrow \{x[n]\} = 1 \). \( \blacksquare \)

Chapter 24.

A2. \( \text{in } \mathbb{Z}_5[x] \)

\[
\frac{x^2 + 3x + 2}{x^2 + x^2 + 6x + 1} \quad q(x) = x - 2 \quad r(x) = 5x + 5
\]

in \( \mathbb{Z}_5[x] \).

\[
\frac{x^2 + 3x + 2}{x^2 + x + 1} \quad q(x) = x + 3 \quad r(x) = 0
\]

B3. Quadratic polynomials in \( \mathbb{Z}_5[x] \):

\( x^2, x^2 + x, x^2 + 2x, x^2 + 3x, x^2 + 4x, x^2 + x + 1, x^2 + x + 2, x^2 + x + 3, \)

\( x^2 + x + 4, x^2 + 2x + 1, x^2 + 2x + 2, \ldots \)

\( \exists a \in \mathbb{Z}_5, b, c, d \in \mathbb{Z}_5 \text{ s.t. } a + b \cdot 5 + c = 0 \) in total possibilities.

Generally, for polynomial of degree \( m \) in \( \mathbb{Z}_n[x] \),

we have \( (n-1)n^{m-1} \) possibilities.

C4. In \( \mathbb{Z}_4 \), let \( a(x) = 2x^2 + x \) \( b(x) = 2x^2 + 1 \)

\( a(x) = 2x^2 + x + b(x) = 2x^2 + 1 \quad (2x^2 + x)(2x^2 + 1) = 4x^4 + 2x^2 + 2x^3 + x = 2x^3 + 2x^2 + x \)

\( \text{deg } ax + bx = 3 < \text{deg } ax + \text{deg } bx = 2 + 2 = 4 \)

In \( \mathbb{Z}_6 \), let \( a(x) = 3x^2 + x \) \( b(x) = 2x^2 + 1 \)

\( a(x) = 3x^2 + x + b(x) = 2x^2 + 1 \quad (3x^2 + x)(2x^2 + 1) = 6x^4 + 2x^3 + 3x^2 + x = 2x^3 + 3x^2 + x \)

\( \text{deg } ax + bx = 3 < \text{deg } ax + \text{deg } bx = 2 + 2 = 4 \)

In \( \mathbb{Z}_9 \), let \( a(x) = 3x^2 + x \) \( b(x) = 3x^2 + x \)

\( a(x) = 3x^2 + x + b(x) = 3x^2 + x \quad (3x^2 + x)(3x^2 + x) = 9x^4 + 3x^3 + 3x^2 + x = 3x^3 + 3x^2 + x \)

\( \text{deg } ax + bx = 3 < \text{deg } ax + \text{deg } bx = 2 + 2 = 4 \)
E4. \( J = \langle p(x) \rangle \) is an ideal of \( A[x] \).

Want to show: \( J \) is an ideal of \( A[x] \).

Define \( \Theta : A[x] \to A \) s.t \( \Theta(p) = p(c_0) \).

Claim: \( \Theta \) is a ring homomorphism.

\[ \Theta(p+q) = \Theta(p) + \Theta(q) \]

\[ \Theta(pq) = \Theta(p) \Theta(q) \]

Without loss of generality, assume \( n \) is m.

\[ \Theta(p(x)) = c_0 + c_1 x + c_2 x^2 + \ldots + c_m x^m \mid x = 0 = c_0 = a_0 b_0 = p(c_0) q(c_0) = \Theta(p) \Theta(q) \]

\[ C_n = \sum_{i=0}^{n} a_i b_i \ldots c_0 = a_0 b_0 \]

\( J = \ker \Theta \) is an ideal of \( A[x] \).

F3. by 1, we know that \( h \) is an onto-homomorphism.

by 2, we know \( \ker h = \langle x \rangle \)

Then \( A[x]/\langle x \rangle \cong A \).

Chapter 25.

A1. \( \Theta \), \( x^2 + 4 = (x^2 + 2)(x^2 - 2) \).

B1. \( x^2 - 4 = (x + 2)(x - 2)(x + 2)(x - 2) \).

C1. Every reducible monic quadratic can be uniquely factored as \( (x + a)(x + b) \).

\( a, b = 0, 1, 2, 3, 4 \).

5. Case for \( a = b \)

C5 case for \( a+b \)

\( C_5 + 5 = \frac{5x^4}{2} + 5 = 15 \).

D1. Let \( ax \), \( bx \) be the generator of \( J \), \( J \) is a nonzero ideal.

When \( J = \langle ax \rangle \), \( bx = ax \cdot c(x) \) for some \( c(x) \in F[x] \).

\[ J = \langle bx \rangle \quad a(x) = bx \cdot d(x) \] for some \( d(x) \in F[x] \).

\[ b(x) = b(x) c(x) d(x) = b(x) [1 - c(x) d(x)] = 0 \quad F \text{ is a field so } F[x] \]

Is an integral domain: \( c(x) d(x) = 1 \), \( \deg c(x) \deg d(x) = \deg c(x) + \deg d(x) = 0 \) \( c(x) = c \) for some \( c \in F \)

\( b(x) = c a(x) \) and \( bx, c a(x) \) are associates.
3. \( \Rightarrow \) Assume \( J \) is a prime ideal, 
\[ J = \langle a(x) \rangle \] 
for some \( a(x) \in J \) such that \( a(x) \) is the polynomial of the lowest degree.

Want: \( a(x) \) is irreducible.

Assume otherwise, then \( a(x) = bx + cx \) \( \in J \) for some \( bx, cx \in J \) of positive degree.

\[ \Rightarrow \] \( J = \langle a(x) \rangle \) for some \( a(x) \in J \) such that \( a(x) \) is irreducible, \( a(x) \) is the polynomial of the lowest degree of \( J \).

For any \( b(x), c(x) \in F[x] \), assume \( b(x)c(x) \in J \)

Want to show: \( b(x) \in J \) or \( c(x) \in J \)

Assume \( bx \in J \).

\[ bx \cdot ax = a(x) \cdot dx \text{ for some } dx \in J \]

\[ a(x) \mid bx \cdot ax \text{ since } bx \in J \text{, } a(x) \mid bx \text{.} \]

\[ a(x) \mid c(x) \Rightarrow c(x) \in J \text{.} \]

4. Let \( J \) be an ideal \( \langle g(x) \rangle \) \( \subseteq \langle p(x) \rangle \) for some \( g(x) \in J \)

Want to show: \( J = F[x] \).

It suffices to show: \( \langle p(x) \rangle \subseteq J \).

\[ p(x) + g(x) = \gcd(p(x), g(x)) = 1 \]

Since \( J \) is an ideal \( J = \langle a(x) \rangle \) for some \( a(x) \in J \)

\[ a(x) = ax \cdot bx \text{ for some } bx \in F[x] \]

\[ p(x) \in J \text{, } p(x) = ax \cdot cx \text{ for some } c(x) \in F[x] \]

\[ a(x) \mid 1 \text{ since } 1 \mid a(x) \text{, } a(x) = c \cdot 1 \text{ for some } c \in F \]

\[ J = \langle c \rangle = F[x] \text{.} \]