5.4.17. If A, B are ideals in a commutative ring R

a) show $A+B = \{a+b \mid a \in A, b \in B\}$ and $AB = \left\{\sum_i a_i b_i \mid a_i \in A, b_i \in B\right\}$ are ideals of R.

It is clear that these are closed under addition and multiplication

Pick $r \in R, c \in A+B$ then $rc = r(a+b) = ra + rb$

since A, B are ideals $ra \in A$, $rb \in B$ so $ra+rb \in A+B$

Pick $r \in R$, $c = \sum_i a_i b_i \in AB$ then $rc = r\sum_i a_i b_i$

$= \sum_i (ra_i) b_i$ since A is an ideal $ra_i \in A$ b_i

so $\sum_i (ra_i) b_i$ is in AB

5.4.17 b) Show that $A+B=R$ implies $AB=A\cap B$

Clearly $AB \subset A\cap B$, so we must show the opposite inclusion

Let $c \in A\cap B$. Since $A+B=R$ we can find

a', b' such that $a'+b'=1$

Then $c = (a'+b')c = a'c + b'c$

Since $c \in A\cap B$, this is an element in AB

5.4.18 Suppose $R = \mathbb{Z}$. If $A = \langle a \rangle$, $B = \langle b \rangle$

Let $c = \gcd(a,b)$ $c = xa + by$, so $\langle c \rangle \subseteq \langle a \rangle + \langle b \rangle$

Conversely for any x', y': $c \mid x'a + y'b$ so

$\langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$

For the second part, by the previous exercise it suffices to prove that $A \cap B = \langle ab \rangle$

But we know from earlier that as subgroups

$A \cap B = \langle ab \rangle$ if $\gcd(a,b) = 1$

Since $A + B = \langle 1 \rangle$, there is x, y s.t. $xa + by = 1$

so $\gcd(a,b)$ must be 1

5.4.20 Suppose F is a field. Find all ideals in F

(0) is an ideal.

Assume $A \neq 0$ is an ideal, and let $0 \neq a \in A$

Then $a^{-1}a = 1 \in A$, so $A = F$

5.4.21 Suppose R, S are rings. What are the ideals in $R \oplus S$?

① If $A \subseteq R$, $B \subseteq S$ are ideals, then $A \oplus B = \{(a,b) \mid a \in A, b \in B\}$ is an ideal of $R \oplus S$

- $A \oplus B$ is clearly a subring.
- Let $(r,s) \in R \oplus S$, then $(r,s)(a,b) = (ra, sb) \in A \oplus B$ and $(a,b) \in A \oplus B$

② If $\mathfrak{J} \subseteq R \oplus S$ is an ideal, then

$A = \{a \mid (a,0) \in \mathfrak{J}\}$ and

$B = \{b \mid (0,b) \in \mathfrak{J}\}$ are ideals in R, S respectively. These are clearly subrings

Let $r \in R$, $a \in A$. Let $(a,b) \in \mathfrak{J}$. Then

$(r,0)(a,b) = (ra, 0) \in \mathfrak{J}$, so $ra \in A$.

Similarly for B.

So the ideals of $R \oplus S$ are precisely $A \oplus B$ for A, B ideals of R, S respectively

Clearly $A \oplus B \subseteq \mathfrak{J}$.

Conversely, let $(r,s) \in \mathfrak{J}$.

then $(1,0)(r,s) = (r,0) \in \mathfrak{J} \Rightarrow r \in A$

and $(0,1)(r,s) = (0,s) \in \mathfrak{J} \Rightarrow s \in B$

so $A \oplus B \supseteq \mathfrak{J}$

Therefor $\mathfrak{J} = A \oplus B$

5.4.22 A non-maximal prime ideal of $\mathbb{Z} \oplus \mathbb{Z}$

is $\langle 1 \rangle \oplus \langle 0 \rangle$

5.5.2. Find the degree 4 irreducible polynomials in $\mathbb{Z}_2[x]$

We follow the technique in the example

Degree 4 polynomials with no constant term

$$x^4+1,\quad x^4+x+1,\quad x^4+x^2+1,\quad x^4+x^2+x+1,\quad x^4+x^3+x^2+1$$

$$x^4+x^3+1,\quad x^4+x^3+x+1,\quad x^4+x^3+x^2+x+1,$$

If the number of terms is even, then the polynomial has a linear factor $x-1$ (Corollary 5.5.1).
This eliminates 8 polynomials
The final case to check is that the polynomial is not a product of two irreducible degree 2 polynomials.

This is only $(x^2+x+1)^2 = x^4+x^2+1$
since there is only one irreducible degree 2 polynomial in $\mathbb{Z}_2[x]$

The remaining 3 polynomials are irreducible

5.5.7. In $\mathbb{Z}_7[x]$ find the quotient and remainder upon dividing $5x^4 + 3x^3 + 1$ by $3x^2 + 2x + 1$

$5x^4 + 3x^3 + 1 : 3x^2 + 2x + 1 \mid 4x^2 + 3x + 6$ — quotient

$-(5x^4 + x^3 + 4x^2)$

$2x^3 + 3x^2 + 1$

$-(2x^3 + 6x^2 + 3x)$

$4x^2 + 4x + 1$

$-(4x^2 + 5x + 6)$

$6x + 1$ — remainder

5.5.11

a) Show that if an ideal A contains a unit, then $A = R$

Let $a \in A$ be a unit. Then $a^{-1}a = 1 \in A$.

Since $1 \in A$, for any $r \in R$ $1 \cdot r = r \in A$

b) See 5.4.20

5.6.1 a) Show that x^2-2 is irreducible in $\mathbb{Z}_5[x]$:

Since x^2-2 has degree 2 it suffices to check that it has no zeros. We check the squares in $\mathbb{Z}_5$ $0^2=0$, $1^2=1$ $2^2=4$ $3^2=4$ $4^2=1$ and see that the polynomial is non-vanishing

b) By corollary 5.5.4 $\mathbb{Z}_5[x]/_{x^2-2}$ is a field.

The cosets correspond 1-1 to polynomials of degree 1 $ax+b$. There are 5 choices each for a and b, so 25 elements.

c) The map $ax+b \mapsto b+a\sqrt{2}$ is an isomorphism

d) The characteristic is 5

5.6.2 Find the powers of $\theta = \sqrt{2}$ with $\mathbb{Z}_5[\sqrt{2}] \simeq \mathbb{Z}_5[x]/x^2-2$

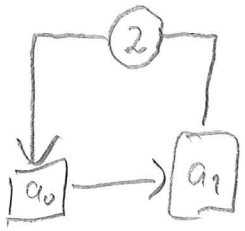
$\theta, 2, 2\theta, 4, 4\theta, 3, 3\theta, 1.$

This is not the whole unit group (which has order 24)

so x^2-2 is not primitive

The feedback-shift-register sends $a_0 + a_1\theta \mapsto 2a_1 + a_0\theta$

$(a_0, a_1) \mapsto (2a_1, a_0)$



5.6.7. a) Show that $\mathbb{Z}_5[i]$ is not a field

Compute $(2-i)(2+i) = 2^2 - i^2 = 4+1 = 0$

Since the ring has zero divisors, it is not a field.

b) $\mathbb{Z}_7[i]$ is a field since x^2+1 is irreducible in $\mathbb{Z}_7[x]$ (it has no zeros)

Therefore $\mathbb{Z}_7[x]/(x^2-1)$ is a field

c) x^2-1 is irreducible in $\mathbb{Z}_p[x]$ iff it has no zeros in $\mathbb{Z}_p$ (prop. 5.5.1)

So $\mathbb{Z}_p[i]$ a field $\Leftrightarrow$ x^2-1 irreducible in $\mathbb{Z}_p[x]$ $\Leftrightarrow$ x^2+1 no zeros in $\mathbb{Z}_p$

$c^2 \equiv -1 \pmod p$ has no solution

So $\mathbb{Z}_p[i]$ is a field $\Leftrightarrow$ $p \not\equiv 1 \bmod 4$ (Using the fact from the exercise)

Proof of the fact from 5.6.7

$c^2 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$

$\mathbb{Z}_p^*$ is cyclic i generates a subgroup of order 4, which is only possible if $|\mathbb{Z}_p^*| = p-1 \equiv 0 \pmod{4}$

Conversely if $|\mathbb{Z}_p^*|$ is divisible by 4, it has a subgroup of order 4. If $\mathbb{Z}_p^* = \langle a \rangle$ and $|\mathbb{Z}_p^*| = n$, then $a^{\frac{n}{2}}$ is the unique order 2 element, so $a^{\frac{n}{2}} = -1$. Hence, $a^{\frac{n}{4}}$ must be i

(a possible choice of)

5.6.11.

a) 2 is a unit so $\langle 2 \rangle = \langle 1 \rangle = \mathbb{Z}_7[x]$

so $\mathbb{Z}_7[x]/\langle 2 \rangle \simeq \{0\}$ Which is (by def.) not a field

b) $\mathbb{Z}_7[x]/\langle x+1 \rangle \simeq \mathbb{Z}_7$ which is a field

c.) $\mathbb{Z}_7[x]/\langle x^2 \rangle$ is not a field since

$[x] \cdot [x] = [x^2] = 0$ so it has zero-divisors.

6.1.3b) Show if A is an ideal of R and $T(R)=S$,

then $T(A)$ is an ideal of S

$T(A)$ is a subring

Since $T(R)=S$ we pick r such that $T(r)=s$

$$sT(a) = T(r)T(a) = T(ra) \in T(A)$$

This is in A since A is an ideal

6.1.6 a) If we try to define $\mathbb{Z}_5 \to \mathbb{Z}_{10}$

by setting $T(x) = 5x$ we do not get a well-defined map

Not well-defined. Let $T: \mathbb{Z} \to \mathbb{Z}$ be defined by $T(x) = 5x$

If $x \equiv y \pmod 5$ e.g. $x = 0$ $y = 5$, then

$5x$ is not necessarily congruent to $5y \bmod 10$

b) Show $T: \mathbb{Z}_4 \to \mathbb{Z}_{12}$ defined by $T(x) = 3x$

is well-defined but not a ring map.

Let $T: \mathbb{Z} \to \mathbb{Z}$ be defined by $x \mapsto 3x$

if $x \equiv y \pmod 4$, then $x = 4n + y$

So $3x = 12n + 3y$, hence $3x \equiv 3y \pmod{12}$

$T(1 \cdot 1) = T(1) = 3$

$T(1) \cdot T(1) = 3 \cdot 3 = 9$

So T does not preserve multiplication.

6.1.6 c)

Let $T: \mathbb{Z}_n \to \mathbb{Z}_n$ be a homomorphism.

Let $a = T(1)$. Then $T(x) = ax$

This is a group homomorphism for any a, so we must only check when it preserves multiplication

$T(xy) = axy$

$T(x)T(y) = ax \cdot ay = a^2xy$

} These are equal for all x, y iff $a \equiv a^2 \pmod{n}$ (pick $x = y = 1$)

For $n = 12$ $9^2 \equiv 9 \pmod{12}$

6.1.12 Show that the only ring automorphism map of $\mathbb{Z}$ is the identity

Let $T: \mathbb{Z} \to \mathbb{Z}$ be a ring automorphism

Any ring automorphism is a group automorphism, so T must send group generators to group generators

The two choices are $T(1) = 1$ and $T(1) = -1$

$T(1) = -1$ is not a ring automorphism since

$$T(1 \cdot 1) = T(1) = -1$$

$$T(1)\,T(1) = (-1) \cdot (-1) = 1$$

6.1.14 Define $T: \mathbb{Z}_{24} \to \mathbb{Z}_{12}$ by

$$x \pmod{24} \longmapsto x \pmod{12}$$

This is well-defined, since if $x = n \cdot 24 + y$, then $x = 2n \cdot 12 + y$

This is a group homomorphism, need to show it respects multiplication:

$$x \pmod{24} \; y \pmod{24} = xy \pmod{24}$$

so

$$T(x \pmod{24}) \, T(y \pmod{24}) = x \pmod{12} \; y \pmod{12}$$

$$= xy \pmod{12} = T(xy \pmod{24})$$

The kernel is $\langle 12 \pmod{24} \rangle$

By the first iso. theorem $\mathbb{Z}_{24}/\langle 12 \rangle \simeq \mathbb{Z}_{12}$