Last time: homomorphisms and unital homomorphism of rings

- degree of polynomials: \( \text{deg}(f \circ g) \leq \text{deg } f + \text{deg } g \)
- Substitution principle: \( \varphi: R \to R' \) (unital) ring homomorphism \( a \in R \), \( \exists ! \varphi(a)x' \) homomorphism \( \varphi_a: R[x] \to R' \)
  so that \( \varphi_a(\sum a_i \cdot x^i) = \sum \varphi(a_i) \cdot x^i. \)

Special cases: \( \varphi_a(\sum a_i x^i) = \sum a_i \varphi(x^i) \)

\[ \begin{align*}
\varphi: R[x] \to R, & \quad \text{ev}_a(\sum a_i x^i) = \sum a_i x^i \quad \text{"evaluation at } x^a" \quad \text{\textendash} \\
\varphi: R \to S \text{ (unital) ring homomorphism, } a = y \in S[y] \to R' \\
\varphi_a: R[x] \to S[y], & \quad \varphi_a(\sum a_i x^i) = \sum \varphi(a_i) y^i. 
\end{align*} \]

Definition. An ideal \( I \) in a ring \( R \) is a subgroup \( I \subseteq (R, +, 0) \) so that for \( r \in R \), \( a \in I \), \( r + a \in I \) and \( r - a \in I \).

\( \exists a \in \mathbb{Z} \) is an ideal: \( \forall r \in \mathbb{Z}, \forall i \in \mathbb{Z}, r \cdot i \in \mathbb{Z} \).

\( \sum a_i x^i \) \( \{0\} \), \( R \) are ideals in \( R \).

Definition. The kernel of a ring homomorphism \( f: R \to R' \) is \( \ker f = \{ r \in R \mid f(r) = 0 \} \).

Proposition 23.1. Let \( f: R \to R' \) be a ring homomorphism. Then \( \ker f \) is an ideal.

Proof. \( I = \ker f \) is a subgroup of \( R \) since \( f: (R, +, 0) \to (R', +, 0) \) is a group homomorphism. Moreover \( \forall r \in R, \forall i \in \mathbb{Z}, r \cdot i \in I \).

\( \sum a_i x^i \) \( \{0\} \) is an ideal in \( R \).

\( \text{Ex} \) \( \pi: \mathbb{Z} \to \mathbb{Z}_n \) is a ring homomorphism. \( n \mathbb{Z} = \ker \pi \) is an ideal in \( \mathbb{Z} \).

\( \text{Ex} \) \( \text{ev}_a: R[x] \to R, \text{ev}_a(\sum a_i x^i) = \sum a_i x^i, \text{ i.e. } p(x) \to p(a) \).
\( \ker(e_{x}) = \{ p(x) \in R[x] \mid p(x) = 0 \} \) is an ideal in \( R[x] \).
It's an ideal of polynomials that are zero at \( x \).

**Definition:** If \( p(x) = 0 \) we say \( x \) is a root of \( p(x) \).

**Example:** \( x + 1 \) is a root of \( p(x) = x^2 + 1 \)

**Example:** If \( p \) is prime, \( a^p = a \) for \( a \in Z_p \)
\( \Rightarrow \forall a \in Z_p \text{ is a root of } q(x) = x^p - x \).

**Note:** The function \( f: Z_p \rightarrow Z_p, \alpha \mapsto a^p - a \) is identically zero,
but \( q(x) = x^p - x \neq 0 \).

**Lemma 23.2:** Let \( I \subseteq R \) be an ideal. If \( 1 \in I \), then \( I = R \).

**Proof:** If \( r \in R \), \( r = r \cdot 1 \in I \).

**Corollary 23.3:** Suppose \( I \subseteq R \) is an ideal and \( u \in I \) is a unit.
Then \( I = R \).

**Proof:** Since \( u \) is a unit, \( \forall v \in R, v \cdot u = 1 \). Since \( u \in I \)
\( 1 = vu \in I \). By 23.2, \( I = R \).

**Corollary 23.4:** If \( F \) is a field and \( I \subseteq F \) is an ideal then
either \( I = \{0\} \) or \( I = F \).

**Proof:** Suppose \( I \subseteq F \) is an ideal and \( I \neq \{0\} \). Then \( \forall u \in I \)
\( \exists v \in F \) s.t. \( u \neq 0 \). Since \( F \) is a field and \( u \neq 0 \), \( \exists v \in F \) s.t. \( uv = 1 \).
\( \Rightarrow u \) is a unit. \( \Rightarrow I = F \).

**Theorem 23.5:** Let \( R \) be a ring and \( I \subseteq R \) an ideal. Then
the quotient group \( (R/I, +, 0) \) has a well-defined multiplication given by
\( (a + I) \cdot (b + I) = (ab) + I \)

With this multiplication \( (R/I, +, \cdot, 0, 1 + I) \) is a ring.
Moreover \( \pi: R \rightarrow R/I \), \( \pi(a) = a+I \) is a (unital) ring homomorphism.

**Sketch of proof:**

1) We check that \( \pi \) is well-defined.

Suppose \( a+I = a'+I \), \( b+I = b'+I \).

We need to check that \( (ab)+I = (a'b')+I \).

Since \( a+I = a'+I \), \( a = a'+i \) for some \( i \in I \).

Since \( b+I = b'+I \), \( b = b'+j \) for some \( j \in I \).

\[
ab - a'b' = (a+i)(b'+j) - a'b' = a'b' + ib + a'i + ij - a'b' = ib + a'i + ij - I.
\]

\[
\therefore \quad ob+I = a'b'+I.
\]

2) \((a+I), \quad ((b+I)+(c+I)) = (a+I), \quad (b+c)+I = (a+b+c)+I = (a+I) \cdot (b+I) + (a+I) \cdot (c+I)\]

Similarly,

\[
((a+I) + (b+I), \quad (c+I)) = (a+I) \cdot (c+I) + (b+I) \cdot (c+I).
\]

3) \((1+I), \quad (a+I) = 1 \cdot a+I = a+I = a \cdot 1 + I = (a+I)(1+I) = 1 \cdot R + I = 1 \cdot R / I.
\]

and so on.

**Exercise:**

Let \( \Phi : R \rightarrow S \) be a (unital) ring homomorphism. Then \( \Phi(1) \) is a subring of \( S \).

**Theorem (1st isomorphism theorem):**

Let \( \Phi : R \rightarrow S \) be a ring homomorphism, and \( I = \ker \Phi \).

Then \( \Phi: R/I \rightarrow S \), \( \Phi(a+I) = \Phi(a) \) is a well-defined injective ring homomorphism. In particular, \( R \rightarrow S \)

\[
\begin{array}{ccc}
R/I & \xrightarrow{\Phi} & S \\
\pi & \\ R/I & \rightarrow & \Phi(R)
\end{array}
\]
and \( \tilde{\varphi} : R/I \to R/\varphi(I) \) is an isomorphism. 

Proof: We know that \( \tilde{\varphi} : R/I \to R, \tilde{\varphi}(a+I) = \varphi(a) \)

in a well-defined isomorphism of abelian groups.

Remains to check: \( \tilde{\varphi} \) preserves multiplication.

Now \( \tilde{\varphi}((a+I)(b+I)) = \tilde{\varphi}(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(a+I)\tilde{\varphi}(b+I) \) \( \square \)

The inclusion \( f : IR \to C, f(a) = a + 0i \) \( \) is an injective, unital

ring homomorphism. By the substitution principle

\( \hat{f} : IR[x] \to C, \hat{f}(\sum_{j=0}^{n} a_j x^j) = \sum_{j=0}^{n} a_j (F_1)^j \) \( \) is a ring homomorphism

\( \hat{f}(a + bx) = a + bF_1. \Rightarrow \hat{f} \) \( \) is onto.

We'll show: ker \( \hat{f} = (x^2 + 1)IR[x] \)

\( = \langle x^2 + 1 \rangle IR[x] \)

1st isomorphism theorem \( \Rightarrow \)

\( C \cong IR[x] / \langle x^2 + 1 \rangle IR[x] \)

Exercise: Let \( \{ I_{a} \}_{a \in A} \) be a collection of ideals in a ring \( R \).

Then \( \bigcap_{a \in A} I_{a} \) is also an ideal in \( R \).

Consequence: Let \( R \) be a ring, \( S \subseteq R \) a set.

Let \( A - \{ I \subseteq R | I \) an ideal and \( S \subseteq I \). Then by exercise

\( \bigcap_{I \in S} A \equiv \bigcap_{I \subseteq R} I \) \( \) is an ideal in \( R \).

Note that \( \forall I \subseteq A, S \subseteq I \Rightarrow S \subseteq \bigcap_{I \in S} A. \)

1. \( \langle S \rangle - \{ \sum_{i} a_i = 0 \} A \) is the smallest ideal containing \( S \). We'll see: if \( R \) is commutative, \( a \in R \) then

\( \langle \{ a \} \rangle = a \langle 1 \rangle = \{ a \} \) for \( 1 \in R \).