Homomorphism theorems for rings

Last time: R a ring, I ≤ R an ideal
Get R/I quotient ring
  \[ \pi : R \to R/I \text{ quotient homomorphism} \]

\[ R/I = \{ r+I \mid r \in R \text{ where } r+I = \{ r + a \mid a \in I \} \]  
\[ (r+I) + (r'+I) = (r+r') + I \]
\[ (r+I)(r'+I) = (rr') + I. \]
\[ \pi(r) = r+I. \]

Observe that if we forget multiplicative, \((R/I, +)\) is the quotient group of \((R, +)\) by \((I, +)\)

Theorem 6.3.4 (Homomorphism theorem for rings)
Let \( \phi : R \to S \) be a surjective homomorphism of rings. Let \( I = \ker(\phi) \), and let \( \pi : R \to R/I \) be the quotient homomorphism. Then there is an isomorphism of rings
\[ \tilde{\phi} : R/I \to S \] such that \( \tilde{\phi} \circ \pi = \phi \)
\[ \tilde{\phi}(r+I) = \phi(r). \]

Proof: If we forget about multiplicative, this is the homomorphism theorem for groups. So we apply that and we get that
\[ \tilde{\phi} : (R/I, +) \to (S, +) \]
\[ \tilde{\phi}(r+I) = \phi(r) \]

is a well-defined isomorphism of groups. To check it is an isomorphism of rings, we just check it respects multiplication:
\[ \tilde{\varphi}(a+I)(b+I) = \tilde{\varphi}(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(a+I) \tilde{\varphi}(b+I). \]

**Example**

There is a homomorphism \( \varphi_i : \mathbb{R}[x] \to \mathbb{C} \)

such that \( \varphi_i(r) = r \) for \( r \in \mathbb{R} \), \( \varphi_i(x) = i \)

(by the substitution principle)

for example, \( \varphi_i(x^3-1) = i^3-1 = -1 - i \).

The homomorphism is surjective since any \( z \in \mathbb{C} \) can be written as \( z = a + bi \) for \( a, b \in \mathbb{R} \), and then

\[ \varphi_i(a + bx) = a + bi = z. \]

By the homomorphism theorem for rings, there is an isomorphism

\[ \tilde{\varphi}_i : \mathbb{R}[x]/I \to \mathbb{C}, \text{where } I = \ker(\varphi_i). \]

What is \( I = \ker(\varphi_i) \)? Certainly \( x^2 + 1 \in \ker(\varphi_i) \),

since \( \varphi_i(x^2 + 1) = i^2 + 1 = -1 + 1 = 0. \)

Because \( \ker(\varphi_i) \) is an ideal, it then also contains all multiples of \( x^2 + 1 \):

\[ (x^2 + 1) = (x^2 + 1)\mathbb{R}[x] = \{ (x^2 + 1)g \mid g \in \mathbb{R}[x] \} \]

and \( (x^2 + 1) \leq \ker(\varphi_i) \)

In fact \( \ker(\varphi_i) = (x^2 + 1) \): Take \( g \in \ker(\varphi_i) \)

Write \( g = (x^2 + 1)p + r \) where \( \deg(r) < \deg(x^2 + 1) = 2 \)

Then \( r = at + bx \) for some \( a, b \in \mathbb{R} \). Now apply \( \varphi_i \)

\[ 0 = \varphi_i(g) = \varphi_i((x^2 + 1)p + at + bx) = \varphi_i((x^2 + 1)p) + \varphi_i(at + bx) \]

\[ = 0 \cdot \varphi_i(p) + at + bi = at + bi \]
So \( a + bi = 0 \) so \( a = b = 0 \) so \( r = 0 \), and \( x^2 + 1 \) divides \( g \).
So \( g \in (x^2 + 1)\mathbb{R}[x] \equiv (x^2 + 1) \).

Thus \( \ker(\psi) \subseteq (x^2 + 1) \) and they are equal.

**Conclusion:** \( \mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C} \) in particular \( \mathbb{R}[x]/(x^2 + 1) \) is a field!

**Proposition 6.3.7** Let \( \varphi: R \rightarrow S \) be a surjective ring homomorphism, and let \( J = \ker(\varphi) \).
For \( B \subseteq S \), consider \( \varphi^{-1}(B) \subseteq R \).
The mapping \( B \rightarrow \varphi^{-1}(B) \) gives a bijection between

\[
\{ \text{subgroups of } (S,+)^2 \} \leftrightarrow \{ \text{subgroups of } (R,+) \text{ containing } J \}^2
\]
\[
\{ \text{subrings of } (S,+) \} \leftrightarrow \{ \text{subrings of } (R,+) \text{ containing } J \}^2
\]
\[
\{ \text{ideals in } (S,+) \} \leftrightarrow \{ \text{ideals in } (R,+) \text{ containing } J \}^2
\]

The statement about subgroups was proved already. It's an exercise to show that the correspondence takes subrings to subrings and ideals to ideals.

**Definition** A **maximal ideal** in a ring \( R \) is an ideal \( M \) such that

- \( M \neq R \)
- If \( I \) is an ideal and \( M \subseteq I \subseteq R \), then either \( I = R \) or \( I = M \).

"There are no proper ideals bigger than \( M \)!!"
Lemma. If $R$ is a ring with 1 and $I \subseteq R$ is an ideal, then $1 \in I \implies I = R$.

Proof. Take any $r \in R$. Then $r \cdot 1 \in I$ since $1 \in I$.

Proposition. Let $R$ be a commutative ring with 1. Assume $1 \neq 0$.

Then $R$ is a field if and only if the only ideals in $R$ are $\{0\}$ and $R$.

Proof. Suppose $R$ is a field. Let $I \subseteq R$ be an ideal. If $I \neq \{0\}$, there is some $a \neq 0$ in $I$. Then $1 = a^{-1}a \in I$ so $I = R$.

Conversely, suppose the only ideals in $R$ are $\{0\}$ and $R$. Let $a \in R$ be a non-zero element. Then $(a) = \{ r \cdot a \mid r \in R \}$ is an ideal in $R$ and $(a) \neq \{0\}$, so $(a) = R$ so $1 \in (a)$ and $1 = r \cdot a$ for some $r \in R$. Then $r$ is a multiplicative inverse for $a$.

Proposition. Let $R$ be a commutative ring with 1. An ideal $M \subseteq R$ is maximal if and only if $R/M$ is a field.

Proof. Consider $\pi : R \to R/M$ there is a bijection

\[
\{ \text{ideals } B \subseteq R/M \} \leftrightarrow \{ \text{ideals } B' \subseteq R \text{ such that } M \subseteq B' \}
\]

\[
B \mapsto \pi^{-1}(B) = B'
\]

$R/M$ is a field $\iff$ only two ideals in $R/M \iff$ only two ideals in $R$ that contain $M$

\[
\{ M/M, R/M \} \quad \overset{?}{\overset{?}{\rightarrow}} \quad M \text{ is maximal.}
\]