Last time "Substitution principle" (6.2.5)

Given a unital ring homomorphism $\varphi : R \to S$ of commutative rings and $a \in S$ $\exists!$ homomorphism $\varphi_a : R[x] \to S$ with

$$\varphi_a\left(\sum_{j=0}^{k} c_j x^j\right) = \sum_{j=0}^{k} \varphi(c_j) a^j .$$

**Proposition 27.1** Let $R$ be a commutative ring (with 1) $a \in R$. Then

$$aR := \{ar \mid r \in R\}$$

is an ideal in $R$.

**Remarks**
- ideals of the form $aR$, $a \in R$, are called principal.
- since $1_R \in R$, $a = a \cdot 1_R \in aR$

**Proof of 27.1** Suppose $x, y \in aR$. Then $\exists\, t, s \in R$ s.t.

$$x = at, \quad y = as.$$

$\Rightarrow$ $x - y = at - as = a \cdot (t - s) \in aR$. $\Rightarrow$ $aR$ is a subgroup

Also, $\forall r \in R$, $r \cdot x = rat = a(rt) \in aR$

$\Rightarrow$ $aR$ is an ideal $\square$

**Ex** $(x^2+1)\mathbb{R}[x] = \{(x^2+1)p(x) \mid p(x) \in \mathbb{R}[x]\}$ is an ideal in $\mathbb{R}[x]$.

**Aside** Given a commutative ring $R$, $R[x]$ is a commutative ring. $\Rightarrow$ $(R[x])[y]$ is again a ring.

An element of $(R[x])[y]$ is $p_0(x) + p_1(x)y + \dots + p_k(x)y^k$ for some $p_0, p_1, \dots, p_k \in R[x]$

Not hard to check

$$(R[x])[y] = \left\{ \sum_{i+j \le k} a_{ij} x^i y^j \;\middle|\; k \ge 0,\ a_{ij} \in R \right\}$$

We usually write $R[x,y]$ for $(R[x])[y]$.

Ex $2\mathbb{Z}[x] = \{2p(x) \mid p(x) \in \mathbb{Z}[x]\}$ is an ideal in $\mathbb{Z}[x]$.

$x\mathbb{Z}[x,y] = \{ x\,p(x,y) \mid p(x,y) \in \mathbb{Z}[x,y]\}$ is an ideal in $\mathbb{Z}[x,y]$.

Proposition 27.2 (compare with 6.2.29) (i) Any ideal in $\mathbb{Z}$ is principal.
(ii) Any ideal in $K[x]$, where $K$ is a field, is principal.

Proof (i) If $I \subseteq \mathbb{Z}$ is an ideal, then $I$ is a subgroup of $(\mathbb{Z},+,0)$.
All subgroups of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 0$.
$\Rightarrow I = n\mathbb{Z}$, i.e. $I$ is principal.

(ii) Let $I \subseteq K[x]$ be an ideal. If $I = \{0\}$, then $I = 0 \cdot K[x]$.
Suppose $I \neq \{0\}$. Then $S = \{\deg h \mid h \in I,\ h \neq 0\} \subseteq \{0,1,2,\ldots,n,\ldots\}$ is non-empty. If $0 \in S$, $0 = \min S$.
If $0 \notin S$, $S \subseteq \mathbb{N}$. Well-ordering $\Rightarrow$ $\min S$ exists.
$\Rightarrow \exists f \in I,\ f \neq 0$ and $\deg f = \min\{\deg h \mid h \in I,\ h \neq 0\}$.
We now argue that $I = fK[x]$.
Since $f \in I$, $fK[x] \subseteq I$.
Now suppose $p \in I$. Division algorithm $\Rightarrow \exists q(x), r(x) \in K[x]$
s.t. $p = q \cdot f + r$ and $\deg r < \deg f = \min(S)$.
Then $r = p - q\cdot f \in I$. Since $\deg r < \min(S)$, $r = 0$.
$\Rightarrow p = q \cdot f \in fK[x]$.
$\Rightarrow I \subseteq fK[x]$.
$\therefore I = fK[x]$. $\square$

Proposition 6.2.23(a) Let $\mathcal{A}$ be some collection of ideals in a ring $R$. Then $\bigcap_{I \in \mathcal{A}} I$ is also an ideal in $R$.

Proof Since each $I \in \mathcal{A}$ is a subgroup of $(R,+,0)$, $\bigcap_{I \in \mathcal{A}} I$ is also a subgroup.

Remains to show: $\forall r \in R$, $\forall x \in \bigcap_{I \in A} I$, $rx, xr \in \bigcap_{I \in A} I$

Since $x \in \bigcap_{I \in A} I$, $x \in I$ for all $I \in A$. Since $I$'s are ideals
$rx, xr \in I$ for all $I \in A$. $\Rightarrow rx, xr \in \bigcap_{I \in A} I$

Consequence Let $S$ be any subset of a ring $R$.
Let $A = \{ I \subseteq R \mid I \text{ an ideal}, S \subseteq I \}$.
Then $\langle S \rangle := \bigcap_{I \in A} I$ is an ideal.
It's called the ideal generated by $S$.

Note (1) If $J \subseteq R$ is an ideal and $S \subseteq J$, then $J \in A$.
$\Rightarrow J \supseteq \bigcap_{I \in A} I = \langle S \rangle$

$\therefore$ (2) $\forall I \in A$, $S \subseteq I$. $\Rightarrow S \subseteq \bigcap_{I \in A} I = \langle S \rangle$.

$\therefore \langle S \rangle$ is the smallest ideal containing $S$.

"Ex" $R$ comm. ring, $a \in R$ $\langle \{a\} \rangle = aR$.

Proposition 6.2.24(b). Let $I, J$ be two ideals in a ring $R$.
Then $I + J = \{ i + j \mid i \in I, j \in J \}$
is an ideal.

Proof Suppose $x_1, x_2 \in I+J$. Then $x_1 = i_1 + j_1$, $x_2 = i_2 + j_2$
for $i_1, i_2 \in I$, $j_1, j_2 \in J$. $\Rightarrow$
$x_1 - x_2 = i_1 + j_1 - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J$.
$\forall r \in R$ $rx_1 = r(i_1 + j_1) = ri_1 + rj_2 \in I+J$
$x_1 \cdot r = (i_1 + j_1) r = i_1 r + j_1 r \in I+J$

$\therefore I+J$ is an ideal.