# Lecture 26 Quotient rings

If $G$ is a group and $N \triangleleft G$ is a normal subgroup, we can form the quotient group $G/N$ and a surjective group homomorphism $\pi : G \to G/N$

$$\pi(a) = aN$$

The parallel story for rings is as follows.
Let $(R, +, \cdot)$ be a ring. An ideal $I \subseteq R$ is a subset such that
- $(I, +)$ is a subgroup of $(R, +)$
- $\forall a \in I, r \in R$, $ar \in I$ and $ra \in I$.

Now $(R, +)$ is an abelian group, so every subgroup is normal. Thus we may form a <u>group</u> $(R/I, +)$

$$R/I = \{ r + I \mid r \in R \} \text{ where } r + I = \{ r + a \mid a \in I \}$$

The addition is $(r + I) + (r' + I) = (r + r') + I$
zero is $0 + I = I$.

This structure makes $R/I$ into an abelian group.
(quotient of an abelian group is abelian).

So far, we have only used the fact that $(I, +)$ is a subgroup of $(R, +)$. To make $R/I$ into a ring, we have to define the multiplication, and that is where we use the second property of an ideal.

We define the multiplication on $R/I$ by

$$(r_1+I)\cdot(r_2+I) = (r_1\cdot r_2)+I.$$

We check it's well-defined: suppose $r_1+I = r_1'+I$
$r_2+I = r_2'+I$.

then $r_1'-r_1 = a_1 \in I$
$r_2'-r_2 = a_2 \in I$.

so $r_1'r_2' = (r_1+a_1)(r_2+a_2) = r_1r_2 + a_1r_2 + r_1a_2 + a_1a_2$

$$r_1'r_2' - r_1r_2 = \underbrace{a_1r_2}_{\in I} + \underbrace{r_1a_2}_{\in I} + \underbrace{a_1a_2}_{\in I} \in I$$
Because $I$ is an ideal.

So $r_1'r_2'+I = r_1r_2+I$, and the definition is consistent.

Proposition $R/I$ is a ring. If $R$ has $1$, then $1+I$ is a multiplicative identity in $R/I$.
If $R$ is commutative, so is $R/I$.
There is a surjective ring homomorphism
$\pi: R \to R/I$ $\quad \pi(r) = r+I$ $\quad$ with $\ker(\pi) = I$
If $R$ has $1$, then $\pi$ is unital.

Example $R=\mathbb{Z}$, $I = n\mathbb{Z} = \{nk \mid k\in\mathbb{Z}\} = \{\ldots,-n,0,n,2n,\ldots\}$
then $R/I = \mathbb{Z}_n$, the ring of congruence classes modulo $n$.
$\pi: \mathbb{Z}\to\mathbb{Z}_n$ $\quad \pi(k) = k+n\mathbb{Z} = [k]_n$

Example $R = K[x]$, $K$ a field. Let $f\in K[x]$ be a nonconstant polynomial, and consider
$I = (f) := fK[x] = \{fg \mid g\in K[x]\}$ = multiples of $f$

This is an ideal in $K[x]$. Consider the quotient $R/I = K[x]/(f)$. We can describe all cosets:
By long division, any $g \in K[x]$ can be written as

$$g = qf + r \quad \text{where } q, r \in K[x] \text{ and } \deg(r) < \deg(f)$$

and $r$ is uniquely determined by these conditions.
Since $qf \in (f)$, we find

$$g + (f) = qf + r + (f) = r + (f)$$

So every coset is of the form $r + (f)$ with $\deg(r) < \deg(f)$
Also, these cosets are distinct for different $r$:
$r + (f) = r' + (f)$ with $\deg(r), \deg(r') < \deg(f)$
$\Rightarrow r - r'$ is divisible by $f$ and
$\deg(r - r') \leq \max(\deg(r), \deg(r')) < \deg(f)$
So $r - r' = 0$ and $r = r'$.

Upshot: every coset in $K[x]/(f)$ has a unique representative $r$ with $\deg(r) < \deg(f)$. We call this the <u>canonical</u> representative.

To add in $K[x]/(f)$: $(r_1 + (f)) + (r_2 + (f)) = (r_1 + r_2) + (f)$
If $\deg(r_1)$ and $\deg(r_2)$ are less than $\deg(f)$, then $\deg(r_1 + r_2) < \deg(f)$

To multiply in $K[x]/(f)$

$$(r_1 + (f))(r_2 + (f)) = r_1 r_2 + (f) = r_3 + (f)$$

where $r_3$ is the remainder of long division of $r_1 r_2$ by $f$.

Example: $K = \mathbb{R}$ $\quad f = x^2+1 \in K[x]$

$$K[x]/(f) = \mathbb{R}[x]/(x^2+1)$$

Canonical representatives are linear (degree 1) polynomials

$$\mathbb{R}[x]/(x^2+1) = \{ a+bx + (f) \mid a,b \in \mathbb{R} \}$$

Addition: $(a+bx+(f)) + (a'+b'x+(f)) = (a+a') + (b+b')x + (f)$

Multiplication: $(a+bx+(f))(a'+b'x+(f))$

$$= aa' + (ab'+a'b)x + bb'x^2 + (f)$$

This is not in canonical form, since it has an $x^2$

We could do long division by $x^2+1$ to reduce it, or we could observe

$$(x^2+1) + (f) = 0 + (f) \quad \text{so}$$

$$x^2 + (f) = -1 + (f)$$

so $aa' + (ab'+a'b)x + bb'x^2 + (f)$

$= aa' + (ab'+a'b)x + bb'(-1) + (f)$

$= (aa'-bb') + (ab'+a'b)x + (f)$

which is in canonical form.

Quick and Dirty way to compute in $K[x]/(f)$:

- Don't write the "$+(f)$" everywhere
- pretend that $f \equiv 0$ is a new rule we are allowed to use to simplify things:

E.g. $K = \mathbb{Q}$, $f = x^3-2$ $\qquad K[x]/(f) = \mathbb{Q}[x]/(x^3-2)$

in $\mathbb{Q}[x]/(x^3-2)$, $\quad x^3 = 2 \quad$ (really $x^3+(f) = 2+(f)$)

so $(2+x+x^2)\cdot(x) = 2x + x^2 + x^3 = 2x + x^2 + 2$

really $(2+x+x^2+(f))(x+(f)) = 2+2x+x^2+(f)$

# Homomorphism theorems for rings

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

**Theorem 6.3.4** (Homomorphism theorem for rings)
Let $\varphi : R \to S$ be a surjective homomorphism of rings. Let $I = \ker(\varphi)$, and let $\pi : R \to R/I$ be the quotient homomorphism. Then there is an isomorphism of rings

$$\tilde{\varphi} : R/I \to S \quad \text{such that} \quad \tilde{\varphi} \circ \pi = \varphi$$

$$\tilde{\varphi}(r+I) = \varphi(r).$$

**Proof** If we forget about multiplication, this is the homomorphism theorem for groups. So we apply that an we get that

$$\tilde{\varphi} : (R/I, +) \to (S, +) \quad \tilde{\varphi}(r+I) = \varphi(r)$$

is a well-defined isomorphism of groups.
To check it is an isomorphism of rings, we just check it respects multiplication:

$$\tilde{\varphi}((a+I)(b+I)) = \tilde{\varphi}(ab+I) = \varphi(ab) = \varphi(a)\varphi(b)$$
$$= \tilde{\varphi}(a+I)\,\tilde{\varphi}(b+I). \qquad \blacksquare$$

**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, $\varphi(x^3 - 1) = i^3 - 1 = -1 - i$.

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
$\tilde{\varphi}_i : \mathbb{R}[x]/I \longrightarrow \mathbb{C}$, 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 $(x^2+1) \subseteq \ker(\varphi_i)$

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 $r = a+bx$ for some $a,b \in r$. Now apply $\varphi_i$

$$0 = \varphi_i(g) = \varphi_i((x^2+1)p + a+bx) = \varphi_i((x^2+1)p) + a+bi$$
$$= 0 \cdot \varphi_i(p) + a+bi = a+bi$$

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

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

<u>Conclusión</u>: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ in particular $\mathbb{R}[x]/(x^2+1)$ is a field!