Ideals (continued)

From last time...

Definition. An **ideal** in a ring R is a subset $I \subset R$ such that

(1) $\langle I, + \rangle$ is a subgroup of $\langle R, + \rangle$, and
(2) $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$. (Here $rI = \{ra : a \in I\}$, $Ir = \{ar : a \in I\}$.)

Therefore the kernel of a ring homomorphism $R \to R'$ is an ideal in R.

Definition. An ideal I in a ring R is **proper** if $I \neq R$.

Definition. Let R be a commutative ring with unity. Then an ideal I in R is **principal** if $I = \langle a \rangle$ for some $a \in R$ (recall that $\langle a \rangle = Ra = \{ra : r \in R\}$).

Remark. Let R be a commutative ring with unity, let I be an ideal in R, and let $a \in R$. Then $a \in I \iff \langle a \rangle \subseteq I$, so $\langle a \rangle$ is the smallest ideal of R that contains a.

Definition. Let R be a commutative ring with unity, and let $a_1, \ldots, a_n \in R$. Then $\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$. It is an ideal in R.

With the above notation, let I be an ideal in R. Then

$$\{a_1, \ldots, a_n\} \subseteq I \iff \langle a_1, \ldots, a_n \rangle \subseteq I .$$

Ideals in $\mathbb{Z}$

Let I be an ideal in $\mathbb{Z}$. Then it's an additive subgroup of $\mathbb{Z}$, so it equals $n\mathbb{Z}$ for some (unique) $n \in \mathbb{N}$.

Conversely, for all $n \in \mathbb{N}$, we have $n\mathbb{Z} = \langle n \rangle$, which is an ideal in $\mathbb{Z}$.

Therefore the set of all ideals in $\mathbb{Z}$ is $\{n\mathbb{Z} : n \in \mathbb{N}\}$, and each ideal is defined by a unique such n.

Moreover, from group theory, we know that if an ideal in $\mathbb{Z}$ is not the zero ideal, then n is the smallest positive element in that ideal.

Proposition. *Let R be a ring with unity 1.*

(a). *Let I be an ideal in R that contains a unit u. Then $I = R$.*
(b). *Assume that R is commutative. Then, for all $a \in \mathbb{R}$, $\langle a \rangle = R$ if and only if a is a unit.*

Proof. (a). For all $a \in R$ we have $u \in I$ and $u^{-1}a \in R$, therefore $a = u(u^{-1}a) \in I$.

(b). If a is a unit then $\langle a \rangle$ contains a unit, so $\langle a \rangle = R$ by the first part. Conversely, if $\langle a \rangle = R$ then $1 \in \langle a \rangle$, so there is a $b \in R$ such that $ab = 1$, and therefore a is a unit. □

Definition. In a ring R with unity, the ideal $I = R$ is called the **unit ideal**.

Corollary. *In a field F, the only ideals are $\{0\}$ and the unit ideal (and they're different).*

Proof. Let I be a nonzero ideal of F. Let u be a nonzero element of I. Then u is a unit, so I is the unit ideal. □

Corollary. *Any nonzero ring homomorphism from a field to a ring is injective.*

Proof. Look at its kernel. □

Quotient (Factor) Rings

Theorem. *Let I be an ideal in a ring R. Then the rules*

$$(a+I)+(b+I)=(a+b)+I \qquad \text{and} \qquad (a+I)(b+I)=(ab)+I$$

give well-defined binary operations on the set R/I of (left) cosets of I in R (under addition), and with these operations R/I is a ring.

Proof. From group theory $+$ (as above) is well defined, and $\langle R/I, +\rangle$ is a group.

To show that multiplication is well defined, suppose $a'+I=a+I$ and $b'+I=b+I$. Then $a'=a+h$ and $b'=b+k$ for some $h,k\in I$, and

$$a'b'-ab=(a+h)(b+k)-ab=ab+ak+h(b+k)-ab=ak+h(b+k)\in I\ ,$$

so $a'b'+I=ab+I$.

Multiplication is associative because

$$((a+I)(b+I))(c+I)=(ab)c+I=a(bc)+I=(a+I)((b+I)(c+I))\ .$$

A similar argument gives the distributive laws, so R/I is a ring. □

Also the canonical map $\gamma\colon R\to R/I$ is a (surjective) ring homomorphism.

Corollary. *All ideals of R occur as kernels of ring homomorphisms.*

Therefore, a subring I of a ring R is an ideal if and only if I is the kernel of a ring homomorphism from R to some other ring.

Also, we have *dissection of a ring homomorphism*: Let $\phi\colon R\to R'$ be a ring homomorphism and let $I=\ker\phi$.

Then ϕ factors as

$$R \xrightarrow[\text{surj.}]{\gamma} R/I \xrightarrow[\sim]{\mu} \phi[R] \xrightarrow[\text{inj.}]{i} R'\ .$$

Proof. We know already that γ is a surjective ring homomorphism. From group theory we know that μ is a bijective group homomorphism, and it is clear that it i is an injective ring homomorphism. Finally, we have

$$\mu((a+I)(b+I))=\mu(ab+I)=\phi(ab)=\phi(a)\phi(b)=\mu(a)\mu(b)\ ,$$

so μ is a ring homomorphism, hence an isomorphism of rings. □

Other Facts

- If R is commutative, then so is R/I.
- If R has unity 1, then R/I has unity $1+I$.
- R/I may have zero divisors even if R does not (example: $R=\mathbb{Z}$, $I=6\mathbb{Z}$).

Key Example: Let $m\in\mathbb{Z}^+$ and apply "dissection" to the map $\phi\colon \mathbb{Z}\to\mathbb{Z}_m$ in the recent handout. Since ϕ is surjective (and has kernel $m\mathbb{Z}$), μ gives an isomorphism $\mathbb{Z}/m\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}_m$. (Here $\mu(n)=r$, where $n=qm+r$ as in the division algorithm.)

Clicker Questions!

Maximal Ideals

Definition. An ideal M in a ring R is **maximal** if it is proper ($M\neq R$) and there is no ideal N of R such that $M\subsetneqq N\subsetneqq R$ (so it is *maximal among proper ideals*).

Examples.

- $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, etc. are maximal ideals in $\mathbb{Z}$ (an ideal N with $p\mathbb{Z}\subsetneqq N\subsetneqq\mathbb{Z}$ would have to be $a\mathbb{Z}$ with $1<a<p$, but $p\mathbb{Z}\subset N$ would require $a\mid p$).
- $\langle 0\rangle$ is a maximal ideal in any field.

Theorem. *Let R be a commutative ring with unity. An ideal M in R is maximal if and only if R/M is a field.*

Proof (uses Ex. 26.22).

Case 1: $M=R$. Then M is not maximal, and $R/M=(0)$ is not a field.

Case 2: $M\neq R$. Then R/M is commutative with $1\neq 0$.

If R/M is not a field then there is an element $a\in R/M$ such that $a\neq 0$ and a is not a unit. Therefore $\langle 0\rangle\subsetneqq\langle a\rangle\subsetneqq R/M$. Letting $\gamma\colon R\to R/M$ be the canonical map (which is surjective), we then have ideals $M=\gamma^{-1}[\langle 0\rangle]\subsetneqq\gamma^{-1}[\langle a\rangle]\subsetneqq\gamma^{-1}[R/M]=R$ in R. This implies that M is not maximal.

Conversely, assume that M is not maximal. Then there is an ideal N of R such that $M\subsetneqq N\subsetneqq R$. Then we have $\gamma[M]\subseteq\gamma[N]\subseteq\gamma[R]$, and these are ideals in R/M.

Pick $a\in N$ such that $a\notin M$. Then $a\notin\ker\gamma$, so $\gamma(a)\neq 0$, which gives $\gamma(a)\notin\gamma[M]=\{0\}$. Therefore $\gamma[M]\neq\gamma[N]$.

Also, if $\gamma[N]=\gamma[R]$ then $\gamma[N]$ contains the element $1+M$, so $1=n+m$ with $n\in N$ and $m\in M$. Since $M\subseteq N$ we have $m\in N$, so $1\in N$ and therefore $N=R$. This is a contradiction, so $\gamma[N]\neq\gamma[R]$.

In conclusion, we have $\langle 0\rangle=\gamma[M]\subsetneqq\gamma[N]\subsetneqq\gamma[R]=R/M$, Therefore R/M is not a field (it has too many ideals). □

[Revisit the set of maximal ideals in $\mathbb{Z}$.]

Prime Ideals

Definition. Let R be a commutative ring. An ideal N in R is **prime** if $N \neq R$ and $ab \in N$ implies $a \in N$ or $b \in N$.

Examples. In $\mathbb{Z}$ the prime ideals are $\langle p \rangle$ with p prime, and $\langle 0 \rangle$.

Theorem. *Let R be a commutative ring with 1. Then an ideal N in R is prime if and only if R/N is an integral domain.*

Proof. First of all, R/N is always commutative and always has unity.

Next, $N \neq R$ if and only if $R/N \neq (0)$, if and only if R/N has $1 \neq 0$.

Finally, we show that the condition

$$(*) \qquad ab \in N \text{ implies } a \in N \text{ or } b \in N$$

is equivalent to R/N not having zero divisors.

" $\Longleftarrow$ ": Suppose that R/N has no zero divisors. Let $a, b \notin N$. Then $a+N$ and $b+N$ are nonzero in R/N, so $(a+N)(b+N) \neq 0$ in R/N, and therefore $ab \notin N$. This shows the contrapositive of (*).

" $\Longrightarrow$ ": We show the contrapositive. Suppose that R/N has zero divisors. Then there are $a, b \in R$ such that $a+N$ and $b+N$ are nonzero in R/N but $(a+N)(b+N) = 0$ in R/N. Then $a, b \notin N$ but $ab \in N$, showing that (*) is false.

In conclusion, N is prime if and only if $N \neq R$ and (*) holds, if and only if R/N has $1 \neq 0$ and R/N has no zero divisors, if and only if R/N is an integral domain (since R/N is commutative by assumption). □

Corollary. *Let R be a commutative ring with 1. Then all maximal ideals in R are prime.*

Proof. Let M be an ideal in R. Then

$$\begin{aligned} M \text{ is maximal} &\iff R/M \text{ is a field} \\ &\implies R/M \text{ is an integral domain} \\ &\iff M \text{ is prime}. \end{aligned}$$

□

Prime Subfields

Proposition. *The characteristic of a field F is either 0 or a prime number, and the field contains a subfield isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$, depending on whether $\operatorname{char} F$ equals 0 or a prime p, respectively.*

Proof. (This was done in the blackboard in class, but I typed it in later for completeness.)

From class on Oct. 29, we have the following.

Let R be a ring with unity 1.

(a). Let $\gamma\colon \langle \mathbb{Z}, + \rangle \to \langle R, + \rangle$ be the unique group homomorphism for which $\gamma(1) = 1$. Then γ is a ring homomorphism $\gamma\colon \mathbb{Z} \to R$.

(b). The characteristic of R is the unique $n \in \mathbb{N}$ such that $\ker \gamma = n\mathbb{Z}$.

Continuing with the proof of the proposition let $n = \operatorname{char} F$. We have two possibilities.

Case 1: $n = 0$. In this case $\gamma\colon \mathbb{Z} \to F$ is injective, so F contains a subring $\gamma[\mathbb{Z}]$ isomorphic to $\mathbb{Z}$. By Theorem 21.6, it follows that F contains a subfield isomorphic to the fraction field of $\mathbb{Z}$, which is $\mathbb{Q}$.

Case 2: $n \neq 0$. In this case (from "dissection of a ring homomorphism" applied to the above map γ), F contains a subring isomorphic to $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, namely $\gamma[\mathbb{Z}]$. We have $n \neq 1$ (because $n = 1$ would imply $1 = 0$ in F) and n is not composite (because in that case $\mathbb{Z}_n$ would have zero divisors, which F does not). Therefore n is a prime number p, and F contains a subring isomorphic to $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field, that subring is a subfield, and we are done. □

Definition. The fields $\mathbb{Q}$ and $\mathbb{Z}_p$ are **prime fields**, and the **prime subfield** of a field F is the (unique) subfield of F as in the above proposition.

Theorem. *Let F be a field. Then every ideal in $F[x]$ is principal.*

Proof. Let N be an ideal in $F[x]$.

Case 1. $N = \{0\}$. Then $N = \langle 0 \rangle$, which is principal.

Case 2. $N \neq \{0\}$. Let $g(x)$ be a nonzero element of N of smallest degree. We claim that $N = \langle g \rangle$. Since $g \in N$, $\langle g \rangle \subseteq N$.

To show $N \subseteq \langle g \rangle$, let $f \in N$ and write $f = qg + r$ with $q, r \in F[x]$ and $\deg r < \deg g$. Then $r = f - qg \in N$, so $r = 0$ (by the assumption on g). Therefore $f = qg \in \langle g \rangle$, so $N \subseteq \langle g \rangle$.

Thus $N = \langle g \rangle$, and therefore N is principal. □

[Compare with the proof for $\mathbb{Z}$ (Theorem 6.6).]