Math 122 Monday, November 21

R = ring (commutative) 1) abelian group under $+$, identity 0
2) commutative, associative multiplication, identity 1
3) $a(b+c) = ab+ac$

e.g. $R = \mathbb{Z}$

Last time showed $0 \cdot a = 0$, $1 \cdot a = a$ $\rightsquigarrow$ If $0 = 1$ then $R = \{0\}$. Otherwise $1 \neq 0$ in R.

$R^\times$ = units of R = $\{a \in R$ for which there is a mult inverse b s.t. $a \cdot b = 1\}$
not closed under addition. e.g. $\mathbb{Z}^\times = \{\pm 1\}$

defn A ring homomorphism is a map $f: R \to R'$ s.t. $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ $\Longrightarrow$ $f(0) = 0'$, $f(1) = 1'$

$\ker f = \{a \in R : f(a) = 0'\} \subset R$ not usually a subring as it may not contain 1
$\operatorname{im} f = \{a' = f(a)\} \subset R'$ is a subring closed under $+$ and $\times$.

defn An ideal $I \subset R$ is a subgroup under $+$ such that $\forall a \in I$, $r \in R$, $ar \in I$.

Claim: $\ker f$ is an ideal. Clearly a subgroup under $+$. If $a \in \ker f$, $r \in R$ then $f(ar) = f(a) \cdot f(r) = 0 \cdot f(r) = 0$ $\Rightarrow$ $ar \in \ker f$.

Prop [As with normal subgroups] Every ideal of R arises as a kernel of a ring homomorphism $f: R \to R'$.

To prove this, given $I \subset R$ construct the quotient ring $R' = R/I$, as the quotient abelian group of cosets of I in R (note R is abelian under $+$ so $I \triangleleft R$ a normal subgroup). Need to define multiplication:

Want to construct a homomorphism $f: R \to R/I$ $a \mapsto a + I$. We know then is a group homomorphism for $+$ with kernel $= I$. If $f(ab) = f(a)f(b)$ must define $(a+I)(b+I) = ab + I$. Is this well defined? Say $a' = a+i$, $b' = b+j$, $i, j \in I$. Then $a'b' = (a+i)(b+j) = ab + ib + aj + ij \in ab + I$ $\Rightarrow$ $ab + I = a'b' + I$.
Hence R/I is a ring and we have in fact the desired ring homomorphism.

ex of ideals $I = \{0\} \subset R$, $I = R \subset R$. Generally given $a \in R$, $I = (a) = \{b = ar : r \in R\}$ the principal ideal generated by a. So $\{0\} = (0)$, $\{1\} = (1)$.

If $R = \mathbb{Z}$ (2) = even integers, $(n) = n\mathbb{Z}$ for each $n \geq 0$. These are the ideals of $\mathbb{Z}$.
$\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is a finite ring with n elements.

In $\mathbb{Z}+\mathbb{Z}i$ the Gaussian integers, every ideal has the form (a). But the ring $\mathbb{Z}+\mathbb{Z}[\sqrt{5}]$ has I of index 2, $I \neq (a)$ by Kummer.

Note: the ring $R=\{0\}$ has only one ideal. Any $R \neq \{0\}$ has at least two ideals: $(0), (1)$.

Thm R is a field $\iff$ R has exactly two ideals.
Pf: Assume $R=F$ is a field. $I \subset R$ with $I \neq (0)$. Take $a \neq 0 \in I$. Let a^{-1} be the multiplicative inverse in R. Then $1 = a a^{-1} \in I \Rightarrow I = (1) = R$. Conversely, assume R has only two ideals (0) and $(1)=R$. Let $a \neq 0$ in R and consider $(a) \neq (0)$. So $(a) = (1) \Rightarrow 1 \in (a) \Rightarrow 1 = a \cdot b$ for some $b \in R \Rightarrow a \in R^\times \Rightarrow R$ a field.

What are ideals in $R = F[x] = \{a_n x^n + \cdots + a_0 \mid a_i \in F\}$, F a field? This is an infinite dimensional F-vector space but also a ring with standard polynomial multiplication.

Thm Every ideal $I = (f(x)) \subset R$ is principal.
Pf: Use Euclidean algorithm for division of polynomials. Claim: If $I \neq 0$ in $F[x]$ then it is generated by any polynomial $f(x) \in I$ of smallest degree. Let $g(x) \in I$. Then $g(x) = m(x) f(x) + r(x)$ for some $m, r \in F[x]$. But $m(x)f(x) \in I$ as $f(x) \in I \Rightarrow r(x) = g(x) - m(x) f(x) \in I$. By Euclidean algorithm can choose m such that $\deg(r) < \deg(f) \Rightarrow r = 0$ as f has smallest positive degree in I. So $g(x) = m(x) f(x) \Rightarrow I = (f(x))$.

defn An R-module M is ① an abelian group under $+$ with identity 0_M
② with scalar multiplication by R, $m \in M$, $r \in R$, $rm \in M$
$r(m+m') = rm + rm'$, $(r+r')m = rm + r'm$

If $R=F$, an R-module is an F-vector space.
If $R=\mathbb{Z}$, an R-module is an abelian group. Define $n \cdot m = \underbrace{m+m+\cdots+m}_{n \text{ times}}$.
For any ring R, both R and any ideal $I \subset R$ are R-modules.

New ex: $R^n = \{(a_1, \ldots, a_n) : a_i \in R\}$ Addition componentwise and $r(a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$
Called the **free**-module of **rank** n.

But, not every R-module is free (i.e., not every R-module has a basis [unlike vector spaces]).

Ex. $n \neq 2$, $M = \mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module but is not free as $\mathbb{Z}^k$ is always infinite.

Turns out an ideal is free iff it is principle.