Math 122 Monday, November 28

$I \subset R$ an ideal = subgroup under $+$, closed under multiplication by R

$a \in R$ $(a) = \{ar : r \in R\}$ principal ideal generated by a. $(0) = \{0\}$ $(1) = R$

$R = \{0\}$ has 1 ideal; any other R has ≥ 2 ideals; R is a field $\Leftrightarrow$ R has only two ideals

For $\mathbb{Z}$ and $F[x]$ the ring of polynomials in one variable with coefficients in a field F, all ideals have the form $(a) = I$. $\begin{cases} a \geq 0 \text{ in } \mathbb{Z} \text{ is the smallest positive element in } I \\ a = f(x) \in F[x] \text{ the monic polynomial of least degree in } I \end{cases}$

$R = F[x,y] = \{\text{polys in two variables}\} = \{a + bx + cy + dx^2 + exy + fy^2 + \cdots\}$ $\quad I = \{bx + cy + dx^2 + exy + fy^2 + \cdots\}$

$f : R \to F$ by $f(x,y) \mapsto f(0,0) = a$ is a ring homomorphism so $\ker f = I$ is an ideal. Note $x, y, x+y \in I$. There is no f s.t. $x = fg$ $y = fh$ so I is not principal. Anything in I can be written as $xf(x,y) + y\,g(x,y)$ so $I = (x,y)$

Notation: $(a_1, \ldots, a_n)$ = smallest ideal containing $a_1, \ldots, a_n = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$

Recall for any ideal I get a quotient ring $\bar{R} = R/I = \{a + I \mid a \in R\}/\sim$ $(a+I)(b+I) = ab + I$

Lattice of all ideals of R is ordered by inclusion $R \supset J \supset I$

J/I = ideal in the quotient ring $R/I = \bar{R}$ = image of J under the homomorphism $f : R \to \bar{R}$
$= \{a + I \mid a \in J\}$ Why an ideal? $(a+I) + (b+I) = (a+b) + I$, $(a+I)(r+I) = ar + I$ ✓

Note there exists a bijection:

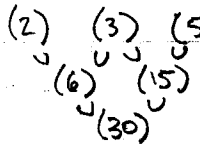
$$\{\text{ideals } J \text{ of } R \text{ containing } I\} \quad \begin{array}{l} J \longmapsto f(J) = \bar{J} \\ J = f^{-1}(\bar{J}) \longleftarrow \bar{J} \end{array} \quad \{\text{ideals } \bar{J} \text{ in } \bar{R} = R/I\}$$

Furthermore: $R/J \simeq \bar{R}/\bar{J}$. How to prove? Consider homomorphism $R \to \bar{R} \to \bar{R}/\bar{J}$ and find the kernel. [Uses the 1st Isomorphism Thm for rings.]

defn We say an ideal $I \subset R$ is maximal if $I \neq R$ (I is a proper ideal) and there are no proper ideals J such that $I \subsetneq J \subsetneq R$.

Prop The ideal I is maximal if and only if R/I is a field.
Pf: Follows immediately from the ideal correspondence.

ex. $R = \mathbb{Z}$ $I = (n)$ $n \geq 0$. $\bar{R} = \mathbb{Z}/n\mathbb{Z}$ is a field only when $n = p$ is prime



For $R=F[x]$ when is $(f(x))=I$ a maximal ideal? If $J=(g(x)) \supsetneq I$ then $f(x)\in(g(x))$ $\Rightarrow f(x)=g(x)\,m(x)$, $\deg g, m > 0$ (if $\deg g=0$ then $J=R$ and if $\deg m=0$ then $I=J$).
So I is maximal $\iff$ $f(x)$ is irreducible in $F[x]$.

e.g. (x^2+1) is maximal in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$. $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ by $x \mapsto i$
More of this when we study Galois theory in Math 123.

$I=(x,y)$ in $F[x,y]$ is maximal because $R/I \xrightarrow{\sim} F$ (a field) by $f(x,y) \longmapsto$ constant term $=f(0,0)$
$(x) \subsetneq (x,y) \subsetneq F[x,y] \Rightarrow (x)$ is not maximal
$R[x,y]/(x) \simeq F[y]$ by $f(x,y) \mapsto f(0,y)$ $y \neq 0$ but has no inverse.

Constructing new rings from old: adjoin elements in a larger ring

Original $R=\mathbb{Q}$ $\quad \alpha \in \mathbb{C}$ $\quad \mathbb{Q}[\alpha]$ = smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and α
$= \{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n \mid a_i \in \mathbb{Q} \}$

$\alpha=2 \Rightarrow \mathbb{Q}[\alpha]=\mathbb{Q}$, $\alpha=i \Rightarrow \mathbb{Q}[\alpha]=\mathbb{Q}+\mathbb{Q}\cdot i$, $\alpha=\pi \Rightarrow \mathbb{Q}[\alpha]$ is a polynomial ring
(π behaves like x because there is no polynomial of finite degree n with rational coefficients satisfied by π)

We say α is algebraic if $\exists f(x) \in \mathbb{Q}[x]$ with $f(\alpha)=0$. In this case, we are interested in the polynomial of smallest degree n satisfied by α (called the minimal polynomial).
If no such f exists, α is transcendental.

Note $\alpha \in \mathbb{Q}$ is surely algebraic as it satisfies $x-\alpha$.

Claim Minimal polynomials are irreducible.
Pf: Say $f(x)=g(x)\,m(x)$. $0=f(\alpha)=g(\alpha)\,m(\alpha) \Rightarrow$ either $g(\alpha)=0$ or $m(\alpha)=0$ but $\deg g, \deg m < \deg f \to\!\leftarrow$. So f is irreducible.

If α is algebraic $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(f(x)) = \mathbb{Q} + \mathbb{Q}x + \cdots + \mathbb{Q}x^{n-1}$ (f minimal poly) is a field which (if you forget the multiplication) is a $\mathbb{Q}$ vector space of dimension n.

e.g. $\mathbb{Q}[i]=\mathbb{Q}[x]/(x^2+1)$, $\mathbb{Q}[\sqrt[3]{2}]=\mathbb{Q}[x]/(x^3-2)$, $\mathbb{Q}[\sqrt[p]{1}]=\mathbb{Q}[x]/(x^{p-1}+x^{p-2}+\cdots+x+1)$ $\left(\frac{x^p-1}{x-1}\right)$

If α is transcendental $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]$ e.g. $\alpha=\pi, e, \gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)$

To study finite fields, we'll consider the quotients $\mathbb{Z}/p\mathbb{Z}[x]/(f(x)) = \mathbb{Z}/p + \mathbb{Z}/p\,x + \cdots + \mathbb{Z}/p\,x^{n-1}$ (f irred of deg $n\geq 1$)
a finite field with p^n elements!
ex. to find a field with p^2 elements it suffices to find an irreducible quadratic polynomial over $\mathbb{Z}/p\mathbb{Z}$. (x^2-a) is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ if a is not a square in $\mathbb{Z}/p\mathbb{Z}$. Claim there are $\frac{p-1}{2}$ non-squares in $(\mathbb{Z}/p\mathbb{Z})^*$. Consider $F:(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ $b \mapsto b^2$ $\ker F=\{\pm 1\}$ of order 2 so image $\simeq (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ has order $\frac{p-1}{2}$.