Lecture 15: Ideals, isomorphism theorems, and examples.

§7-11 of [R2]
§7.2-3 of [DF].

Previously ...

R ring with 1.

$I \subseteq R$ is a (2-sided) ideal when

a) I is a subgp of $(R,+)$.

b) $r \cdot I \subseteq I$ and $I \cdot r \subseteq I$ for all $r \in R$.

Ex: $\phi: R \to S$ a ring hom, $I = \ker(\phi)$.

For any (2-sided) ideal I, can make R/I (quotient of $I \leq (R,+)$) into a ring by $(a+I)(b+I) = ab+I$.

If $\pi: R \to R/I$ is the quo hom $r \mapsto r+I$, then $\ker(\pi) = I$. So ideals in R are analogous to $N \trianglelefteq G$. [Gives analogues of hom/isom thms.].

Lemma: $\phi: R \to S$ a ring hom, $I \subseteq R$ an ideal. If $I \subseteq \ker\phi$, $\exists!$ ring hom $\bar{\phi}: R/I \to S$ such that $\phi = \pi \circ \bar{\phi}$.

Thm: $\phi: R \to S$ a ring hom. Then $R/\ker(\phi) \cong \operatorname{im}(\phi)$ as rings.

[To prove, apply the version for groups to $I \leq (R,+)$ and check that $\bar{\phi}$ is a ring hom as $\bar{\phi}(a+I) = \phi(a)$.]

$D \neq 0$ in $\mathbb{Z}$ squarefree (no p^2 divides D for prime p).

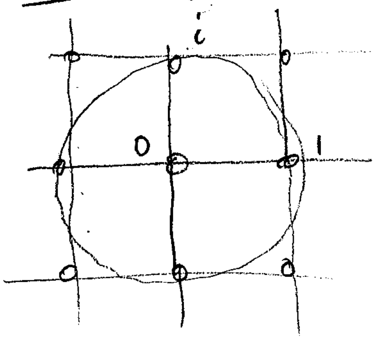
$$\mathbb{Q}(\sqrt{D}) := \{ a + b\sqrt{D} \in \mathbb{C} \mid a, b \in \mathbb{Q} \}$$

This subring of $\mathbb{C}$ is itself a field as

$$(a+b\sqrt{D})^{-1} = \frac{1}{a+b\sqrt{D}} \cdot \frac{a-b\sqrt{D}}{a-b\sqrt{D}} = \frac{a-b\sqrt{D}}{a^2-b^2D} \in \mathbb{Q}(\sqrt{D})$$

$\mathbb{Z}[\sqrt{D}] = \{ a + b\sqrt{D} \mid a, b \in \mathbb{Z} \}$ a subring.

<u>Ex</u>: $R = \mathbb{Z}[i]$ $\quad R^\times = \{1, -1, i, -i\}$ since if $r, s \in R$ with $rs = 1$ then $|r| \cdot |s| = 1$ where $|a+bi| = \sqrt{a^2+b^2} \geq 1$ is the usual complex abs. val. So $|r| = 1$.



<u>Ex</u>: $R = \mathbb{Z}[\sqrt{2}]$ $\quad R^\times = \{ \pm (1+\sqrt{2})^n \mid n \in \mathbb{Z} \}$

When $D \equiv 1 \bmod 4$, can expand $\mathbb{Z}[\sqrt{D}]$ to a larger subring. The <u>ring of integers</u> in $\mathbb{Q}(\sqrt{D})$ is

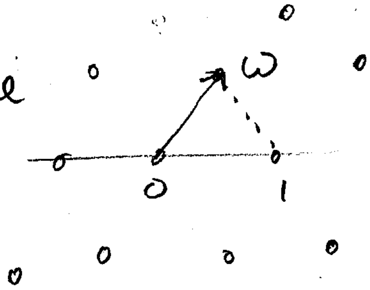
$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} := \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{for } D \equiv 2, 3 \bmod 4 \\ \mathbb{Z}\left[\omega = \frac{1+\sqrt{D}}{2}\right] & \text{for } D \equiv 1 \bmod 4. \end{cases}$$

root of $X^2 - X + \frac{(D-1)}{4}$

<u>Note</u>: In 2nd case $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is in $\mathcal{O} \iff a - b \in \mathbb{Z}$ and $2a \in \mathbb{Z}$.

Ex: $D=-3$, so $\omega = \frac{1+\sqrt{-3}}{2} = \frac{1+\sqrt{3}\,i}{2}$

has $\omega^6 = 1$, and $\mathbb{Z}[\omega] \subseteq \mathbb{C}$ is the hexagonal lattice [Called the Eisenstein ints.]



Moral: Every $z \in \mathbb{Q}(\sqrt{D})$ satisfies a poly with integer coeffs. $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is the subset where the polys are monic. (leading coeff $=1$).

The norm map $N: \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ is

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2 D$$

Props: $N(\alpha) = 0 \iff \alpha = 0$

$N(\alpha\beta) = N(\alpha)N(\beta)$

$\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \Rightarrow N(\alpha) \in \mathbb{Z}$.

$\alpha \in \mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{D})} \iff N(\alpha) = \pm 1$.

$\boxed{\text{When } D<0,\ N(\alpha) = |\alpha|^2}$

Pf of last: (skip!) $(\Rightarrow)$ follows as N is multiplicative, so takes units to units. $(\Leftarrow)$ For $\alpha = a+b\sqrt{D}$, use $\alpha^{-1} = \frac{a-b\sqrt{D}}{N(\alpha)}$. ▨

[Norm is super-useful e.g. for detecting irred. elts.]

G group, R comm. ring with 1.

The <u>group ring</u> $R[G]$ is the ring whose elts are "finite formal sums" $\sum_{g \in G} a_g \cdot g$ with $a_g \in G$ and all but finitely many a_g nonzero. Addition is component-wise, and mult is determined by the distributive law and $(a_g \cdot g) \cdot (a_h h) = (a_g a_h)(gh)$.

<u>Ex</u>: $G = C_2 = \langle x \mid x^2 \rangle \quad R = \mathbb{Z}$.

$r_1 = 2 \cdot e + 3x \qquad r_2 = 5e + 2x$

$r_1 + r_2 = 7e + 5x \qquad r_1 \cdot r_2 = (10e + 4x + 15x + 6e)$
$= 16e + 19x$.

Has 0-divisors

$(e + x)(e + (-1)x) = e + (-1)x + x + (-1)e$
$= 0$.

Note: When G is nonabelian $R[G]$ is not commutative.

Kaplansky Conjecture (1950s) If G is torsion-free and $\mathbb{F}$ a field, then $\mathbb{F}[G]$ has no zero-divisors.

Known for free groups and solvable groups.