Title

Contents

1 | October 20th, 2017

Theorem: If you have a Dedekind ring, on the level of ideals there is unique factorization. R dedekind, $I \neq 0$ then I factors uniquely into prime ideals.

Main Lemma: Take p maximal, then $p^{-1}I \neq I$. $I^{-1} = \{x \in K \mid xI \in R\}$ a fractional ideal.

Corollary: p prime implies $p^{-1}p = R$ Proof: $p \subsetneq p^{-1}p \subseteq R$. But P is maximal.

Proof

Uniqueness:

Suppose $I = p_1 \cdots p_r = q_1 \cdots q_s$. Then $I \subseteq p_1$. So some $q_i \in p_1$. Reorder such that $p_1 = q_1$, multiply by p_1^{-1} Using the corollary above, repeat inductively.

Existence:

Let $\Sigma = \{I \text{ without prime factorization}\} \neq 0$. Since R is noetherian, choose $J \in \Sigma$ a maximal element. $J \neq R$, and $J \subseteq p$ a maximal ideal. Then $Jp^{-1} \subseteq pp^{-1} = R$. By the lemma, $J \subsetneq Jp^{-1}$. Using corollary, show $Jp^{-1} \notin \Sigma, Jp^{-1} = p_2 \cdots p_r$. so $J = pp_2 \cdots p_r \notin \Sigma$. □

Corollary:

$I^{-1}I = R$. (Really is the group-theoretic inverse, so $(IJ)^{-1} = J^{-1}I^{-1}$ etc)

Proof: $I = p_1 \cdots p_r$, check that $I^{-1}I = p_1^{-1} \cdots p_r^{-1}$.

$\text{div}(R) = \{\text{fractional nonzero ideals}\}$ is a free abelian group on the maximal ideals, so $\cong \oplus_p \mathbb{Z}$.

"To contain is to divide", i.e. $I, J \in R$ and $I \subset J \Rightarrow J \mid I$ so $J = II'$. Exercise: $IJ = I \cap J$.

Corollary

1. $0 \neq I \subset J$ then $J = I + (x)$ for some $x \in R$.
2. I an ideal,$\forall 0 \neq a \in I, I = (a, b)$ for some $b \in I$.
3. $I \neq 0$, then there exists $0 \neq I^*$ such that II^* is principal. Can take I^* coprime to I.

Proof

1. Let $I = \Pi p_i^{a_i}$ and $J = \Pi p_i^{b_i}$. Since $J \mid I, b_i \leq a_i$ for all i. For each i, pick $x_i \in p_i^{b_i} - p_i^{b_{i+1}}$. By CRT, $\exists x \in R \mid x = x_i \mod p_i^{a_i}$ since $p_i^{a_i} + p_j^{a_j} = R$ when $i \neq j$. Then $I + (x) \subset J$. But $I + (x) = \Pi p_i^{c_i}, b_i \leq c_i \leq a_i$, forcing $c_i = b_i$.

2. ?
3. Pick any $a \in I$, then $(a) = \Pi p_i^{d_i}$ and $I = \Pi p_i^{a_i}$ where $d_i \geq a_i$. Then take the integral ideal $I^* = \Pi p_i^{d_i - a_i} \subset R$, and modify it to make it coprime to I. How? We're given J, and $IJ \subset I$ and by (1), $I = IJ + (x)$. So $(x) \subset I$ and $(x) = II^*$. Claim: I^* is coprime to J. Proof: $IJ + II^* = I$, multiply by I^{-1} to obtain $J + I = R$.

Theorem

$\mathrm{div}(R) = \oplus_p \mathbb{Z}$ is a free abelian group, $P(R) = \{xR : x \in K^\times\}$ is a subgroup, so ideal class group $\mathrm{Cl}(R) := \mathrm{Div}(R)/P(R)$: every abelian group is the idea class group for some dedekind ring R.

Example: Let $R = \mathbb{C}[x,y]/(y^2 - x^3 - ax - b)$. Then $\mathrm{Cl}(R)$ is uncountable (see Jacobian?). But for number fields, the class group is finite.

Theorem

K a number field, $\mathrm{Cl}_K = \mathrm{Cl}(\mathcal{O}_K)$ is a *finite* group. The order of the group is called the **class number**, measures the failure of unique factorization (h_K). $h_K = 1 \iff \mathcal{O}_K$ PID $\iff \mathcal{O}$ UFD.

Theorem

$\exists M > 0$ such that every nonzero $I \subset \mathcal{O}_K$ contains some $\alpha \neq 0$ such that $|N(\alpha)| \leq M.N(I)$

Corollary

Every ideal class in $\mathcal{O}_K$ contains a nonzero ideal I with $N(I) \leq M$, so $h_K < \infty$. Why? Only finitely many ideals satisfying this condition! $N(I) = m, m\mathcal{O}_K \subset I, \mathcal{O}_K/m\mathcal{O}_K$.

Proof: For $c\ in \mathrm{Cl}_K$, say $c^{-1} = [I]$ with $I \in \mathcal{O}_K$. Pick $\alpha \neq 0$ in I such that $|N(\alpha)| \leq M.N(I)$. $(\alpha) \subset I, (\alpha) = IJ$ for some J, so $[J] = [I]^{-1} = c$, so $N(J) = N((\alpha))N(I)^{-1}$ since the norm is multiplicative. So $N(J) = N(\alpha)N(I)^{-1} \leq M$ (not obvious that norm of ideal is norm of generator).

Will be able to compute M explicitly (the Minkowski bound).

2 | October 25th , 2017 (?)

Theorem Let k be a number field, $n = [k : Q]$.

Then $\exists M > 0$ such that every nonzero ideal $I \in O_k$ contains and $\alpha \neq 0$ such that $|N(\alpha)| \leq MN(I)$.

Proof Pick a $\mathbb{Z}$ basis $\{\alpha_i\}^n$ for O_k. Let $m \geq 1$ be an integer such that $m^n \leq N(I) \leq (m+1)^n$. Define $\Sigma = \{\sum m_j \alpha_j \,\Big|\, 0 \leq m_j \leq m\} \subseteq O_k$.

Then $\#\Sigma = (m+1)^n > N(I)$ by pigeonhole principle. So there exist $x, y \in \Sigma, x \neq y, x - y \in I$.

Claim: Take $\alpha := x - y$, this works. Why? $\alpha = \sum_{j=1}^{n} m_j \alpha_j$, where $|m_j| \leq m$.

Then

$$N(\alpha) = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j||\sigma_i(\alpha_j)| \leq m^n \prod \sum |\sigma_i(\alpha_j)| \leq MN(I)$$

, where the last sum/product term equals M, depending on choice of basis.

$\blacksquare$

Corollary

Every ideal class in Cl_k contains an ideal $I \in O_k$ with $N(I) \leq M$.

Proof $c = [J]^{-1}$ some $J \in O_k$, apply theorem to J. So $\exists \alpha \neq 0 \in J$ where $|N(\alpha)| \leq MN(J)$. So $(\alpha) = JI$ for some $I \in O_k$, works since $(I \in c)$, and $[1] = [J][I]$.

Corollary $h_k < \infty$, take $c_i \in \mathrm{Cl}_k, c_i \in I_i$ with $N(I_i) \leq M$. There are only finitely many $I \in O_k$ with $N(I) = m$. Why? $mO_k \in I, O_k/mO_k$ is finite.

Example $k = Q(\sqrt{d})$, d squarefree. If $d \neq 1 \mod 4$ then $O(k) = Z[\sqrt{d}], d_k = 4d$. Then $M_1 = (1 + |\sqrt{d}|)(1 - |\sqrt{d}|) = (1 + \sqrt{|d|})^2$. $M_2 = \dfrac{2}{4}(\dfrac{4}{\pi})^2\sqrt{4|d|}$, so $\sqrt{d}$ if $d > 0$, else $(4/\pi)\sqrt{|d|}$.

Theorem Take $k \in Q(\alpha), \alpha \in O_k$ an algebraic integer. Suppose $p \not| [O_k : Z[\alpha]]$. Then factor the minimal polynomial $\overline{f_\alpha}$ into irreducibles:

$\overline{f_\alpha}(x) = \overline{h_1}(x)^{e_1} \cdots \overline{h_t}(x)^{e_t}$. Choose lifts $h_i \in Z[x]$, then

$(p) = pO_k = p_1^{e_1} \cdots p_t^{e_t}$ where $p_i = (p, h_i(\alpha))$ and $f_i = \deg(h_i)$.

(That is, factor minimal polynomial mod p and read off.)

Example: Claim: $k = Q(\sqrt{2})$ has class number $h_k = 1$. Note $O_k = Z[\sqrt{2}]$ is a UFD. $M_1 = (1 + \sqrt{2})^2 \approx 5.82 < 6$, $M_2 = \sqrt{2} < 2$, so $h_k = 1$. Can check that $x^2 - 2$ is irreducible mod $p = 3, 5$. But $p = 2$ yields $(2) = (\sqrt{2})^2$. Theorem tells you $p = 3, 5$ are inert. Norms are 9, 25.

Since $N(I) \leq M_1$, we must have $I = (1), (\sqrt{2}), (2)$ of norms $1, 2, 4$, but these are all principal, so every ideal class is trivial.

Example $k = Q(\sqrt{-5})$ has $h_k = 2$. $O_k = Z[\sqrt{-5}]$ and $d_k = 4(-5) = -20$. $M_1 = (1 + \sqrt{5})^2 < 11$ $M_2 = (4/\pi)\sqrt{5} < 3$ (Minkowski bound)

So just need to worry about $p = 2$. Look at $f(x) = x^2 + 5 \mod 2 = (x + 1)^2 \mod 2Z[x]$, then $(2) = p^2, p = (2, 1 + \sqrt{-5})$. But p is not principal - why?

Suppose it is, then $p = (\alpha)$ and $2 = N(p) = |N(\alpha)| = a^2 + 5b^2$ which has no solutions.

So generally, using Minkowski bound gives $N(I) \leq M_2 \iff I = (1)$ or (p).

Theorem $y^2 = x^3 - 5$ has no solutions over Z.

Proof:

Observation: x must be odd, else $y^2 = -1 \mod 4$.

Observation: x, y coprime. If $d|x$ and $d|y$ then $d = 5$, but read equation mod 25.

Factor in $Z[\sqrt{-5}]$, equals $x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5})$, coprime. Why?

Suppose there is a prime ideal p dividing both. Then p divides the sum, so $2y \in p$. But p divides (x), so $x \in p$, thus $\mathrm{GCD}(2y, x) = 1$ which is a contradiction.

So $(y+\sqrt{-5}) = a^3, (y-\sqrt{-5}) = b^3$ for some integral ideals a, b. But the class number is 2 from earlier calculation, so $[a] = [a^3] = [(1)]$ so a must be principal (same goes for b). So choose a generator, $a = (a+b\sqrt{-5})$, generators are same up to a unit.

Then $y+\sqrt{-5} = (a+b\sqrt{-5})^3 = (a^3-15ab^2)+(3a^2b-5b^3)\sqrt{-5}$. So $b = \pm 1$ by equating components, but $3a^2-5 = \pm 1$ has no solutions. $\square$

Similar arguments will be mimicked for Fermat's Last Theorem.

2.1 Bonus

Define Grothendieck group of a ring (k theory) $K_O(O_k) = Z \oplus \mathrm{Cl}_k$. Monoid of finite projective modules, modded out by stuff. $[P]+[Q] = [P \oplus Q]$.

If R is Dedekind,

- Every fractional ideal is a finitely generated projective module
- Every f.g. proj. module $a_1 \oplus \cdots \oplus a_r$ a fractional ideal.

Theorem from Steinitz:

If $a_1 \oplus \cdots a_r \cong b_1 \oplus \cdots b_s$ then $r = s$ and ideal classes are the same.

Using theorem, apply map $[a_1 \oplus \cdots a_r] \mapsto (r, [a_1 \cdots a_r])$

3 | November 11th, 2017

3.1 Fermat's Last Theorem

First case, due to Kumar. Here's what we'll show:

Theorem: Take a prime $p > 3$, assume p is *regular* (i.e. $p \not| h_{\mathbb{Q}(\zeta_p)}$the class number). Then $x^p + y^p = z^p \implies xyz = 0 \mod p$.

Kummer's Criterion: p is irregular (so $p \mid h_{\mathbb{Q}(\zeta_p)}$) iff $\mathrm{ord}_p(B_k) > 0$ for some $k = 2, 3, \cdots p-3$, where B_k is a Bernoulli Number. $\dfrac{z}{e^z-1} = \sum_{n=0}^{\infty} B_n \dfrac{z^n}{n!}, |z| < 2\pi$.

Infinitely many irregular - known, 39%

Infinitely many regular - open, 61%

Herbrand-Ribet:

$A = \mathrm{Cl}_{\mathbb{Q}(\zeta_p)}, C = A/A^p$ is an $\mathbb{F}_p$ vector space where $C = 0 \iff p \not| h$.

$G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, so its dual group is also cyclic $\widehat{G} =< x >$ where $X \cdot G \to \mathbb{F}_p^\times$ is the cyclotomic character $X(\sigma) = [a]$ if $\sigma(\zeta_p) = \zeta_p^a$.

So fix an even $2 \le k \le p-3$. Then $\mathrm{ord}_p(B_k) > 0 \iff C(X^{1-k}) \neq 0$. (Only known to be iff this past century!) Was known assuming Vandiver's conjecture: $p \not| h_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}$. Ribet was able to bypass using Galois representations associated to modular forms. Under this assumption, create a cusp form congruent to an Eisenstein series $\mod p$. Move back into Galois side to recover nontriviality on RHS.

Idea: Factor both sides in the cyclotomic field, so really need to know units in these fields.

There is a natural notion (intrinsic) of conjugation on the cyclotomic field. Take $K_n = \mathbb{Q}(\zeta), \mathrm{ord}(\zeta) = n, \zeta \in \overline{\mathbb{Q}}$.

Then $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ by $c \mapsto [-1]$. Notate by $x \mapsto c(x)$.

Then $c(\zeta) = \zeta^{-1}$, nd for all $\sigma : K_n \to \mathbb{C}, \sigma(\zeta) = e^{2\pi ikn}$ with $\gcd(k, n) = 1$.

So $\sigma(\zeta^{-1}) = \overline{\sigma(\zeta)}$

and $\sigma \circ c = \bar{\sigma} = (\text{conjugation}) \circ \sigma$

Kronecker's Lemma: Take $\alpha \in \overline{\mathbb{Z}}/\{0\}, |\sigma(\alpha)| \leq 1$ for all $\sigma : \overline{\mathbb{Q}} \to \mathbb{C}$. Then α is a root of unity.

Proof: $f(x) = \mathrm{Irr}(\alpha, \mathbb{Q}, x) \in \mathbb{Z}[x]$. $n = \deg(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then $a_m = \pm \sum_{j \leq m} \alpha_{i_j}, |a_m| \leq \binom{n}{m}$. But only finitely many $f(x) \in \mathbb{Z}[x]$ satisfy $\deg(f) \leq n$. Thus there are only finitely many $\alpha \in \overline{\mathbb{Z}}$ that satisfy $\deg(f_\alpha) \leq n$.

Note that α^k satisfies the hypothesis, $f_\alpha k$ satisfies the bounds and $\deg f_\alpha k \leq n$.

Proposition (Kummer): $p > 2$ prime,$u \in \mathbb{Z}[\zeta_p]^\times$. Then $u/\bar{u} = \zeta_p^k$ for some $k \in \mathbb{Z}$.

Lemma: $\alpha \in \mathbb{Z}[\zeta_p]$, then $\exists a \in \mathbb{Z}$ such that $\alpha^p = a \mod (p)$.

Proof: $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, $a^p = \sum_{i=0}^{p-2} a_i \mod (p)$ where $a \in \mathbb{Z}$.

Lemma: $\mu_\infty(K) = \cup \mu_n(K) = (K^\times)_{\text{torsion}}$. Then $\mu_\infty(\mathbb{Q}(\zeta_n)) =< (-1)^m \zeta_n >$ where $m := n \mod 2$.

Proof(Kummer): Take $\alpha = u/\bar{u} \in \mathbb{Z}[\zeta_p]$. Then $\sigma(\alpha) = \sigma(u)/\bar{\sigma}(u) \in \mathbb{C}^d$. By Kronecker, $\alpha = \pm\zeta_p^k$. Claim: sign $= \pm 1$. Otherwise, $u^p = -\bar{u}^p$.

By other lemma, $\exists a \in \mathbb{Z} \;\Big|\; u^p = a \mod (p) \iff \bar{u}^p = a \mod (p) \iff a = -a \mod p$. But then $p \;\Big|\; a$, so $p \;\Big|\; u^p$ and p is a unit. So $|N(p)| > 1$.

Corollary: Every unit $u \in \mathbb{Z}[\zeta_p]^\times$ for $p > 2$ factors as $u = v \cdot \zeta_p^k$ where$v \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$ for some $0 \leq k \leq p$.

Proof: Know from proposition that $u/\bar{u} = \zeta_p^{k'}$, so find $0 \leq k \leq p$ such that $2k = k' \mod p$. Then $u\zeta^{-k} = \bar{u}\zeta_p^{k'-k} = \bar{u}\zeta_p^k$, so take $v = u$ and $\bar{u}\zeta_p^k = \bar{v}$.

Note that $\mathbb{Q}(\zeta + \zeta^{-1})$ is totally real (see midterm!), so $\mathcal{O}_{\mathbb{Q}(\zeta+\zeta^{-1})} = \mathbb{Z}[\zeta + \zeta^{-1}]$.

CM Field: K over K^+ (s), K^+ over $\mathbb{Q}$ totally real. Then $U_k = \mathcal{O}_K^\times$. So define $Q := [U_k : \mu(k)U_{K^+}] \leq 2$. Why? Let $u \in U_k$, then take a complex embedding $\sigma(u/\bar{u}) \in \mathbb{C}^1$. Then consider $U_k \to \mu(K)/\mu(K)^2 \cong \mathbb{Z}/2\mathbb{Z}$ where$u \mapsto [u/\bar{u}]$, which is a homomorphism. The isomorphism follows from $\mu(K)$ being finite and cyclic.

Then $\ker\varphi = \mu(K)U_{K^+}$. The LTR inclusion is from $u/\bar{u} = \zeta^2$, then $u\zeta^{-1} = \bar{u}\zeta = \overline{u\zeta^{-1}}$.

Can show $Q = 1$ for $K = \mathbb{Q}(\zeta_n), n = p^r$ (i.e. n is any prime power), and $Q = 2$ when n is not a prime power and $n \neq 2$. This uses the fact that $1 - \zeta_n$ is a unit when $n \neq p^r$.