Number Fields recap

Seb Millar

June 1, 2018

1 Lectures

1. Number Field (NF) is alg extn of $\mathbb{Q}$, lemmas from Galois, Gauss: $c(fg) = c(f)c(g)$, α is alg integer if min poly/$\mathbb{Z}$ is monic

2. Def of alg integers, main result: $\mathcal{O}_K$ is a ring! (prf:classn of f.g. $\mathbb{Z}$-modules, torsion free by lagrange, Cay-Ham to find poly), $\exists n$ st $n\alpha \in \mathcal{O}_L$ (proj), fund lemma of gal

3. Def $r + 2s$, $\mathrm{Tr}_{L/K}$, $\mathrm{N}_{L/K}$ show theyre additive/multve over extenstions resp. $\sigma_0\left(\mathrm{Tr}_{L/K}(\alpha)\right) = \sum \sigma_i(\alpha)$, $\sigma_0\left(\mathrm{N}_{L/K}(\alpha)\right) = \prod \sigma_i(\alpha)$ for extns $\sigma_1, .., \sigma_{\mathrm{n}} : L \to \mathbb{C}$ of embedding $\sigma_0 : K \to \mathbb{C}$. Cor: $\alpha \in \mathcal{O}_L \Rightarrow \mathrm{N}_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$, use to classify quadtc fields:

   (a) $d \equiv 2, 3(\mathrm{mod} 4)$ squarefree $\Rightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$

   (b) $d \equiv 1(\mathrm{mod} 4)$ squarefree $\Rightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$

4. $\mathcal{O}_L^* = \{\alpha : \mathrm{N}(\alpha) = \pm 1\}$. Def of $\mathrm{disc}(\alpha_1, .., \alpha_n)$ as $\det^2$ of all embeddings of α_i, def $T_{ij} = \det(\alpha_i\alpha_j)$, show $\det T = \mathrm{disc}(\alpha_1, .., \alpha_{\mathrm{n}})$, so $\alpha_i \in \mathcal{O}_L \Rightarrow \mathrm{disc}(\alpha_1, .., \alpha_{\mathrm{n}}) \in \mathcal{O}_K$. non-zero disc implies α_i form $\mathbb{Q}$-basis for L, (since non-zero disc means T inv so $\mathrm{Tr} : (x, y) \mapsto \mathrm{Tr}_{L/\mathbb{Q}}(xy)$ is non-degen symm bilinear form). def int basis as $\mathbb{Z}$-basis, show $(\alpha_1, .., \alpha_{\mathrm{n}})$ int basis $\Rightarrow$ ($\mathbb{Z}^n \to \mathcal{O}_L$, $(m_1, .., m_n) \mapsto m_1\alpha_1 + .. + m_n\alpha_n$ is isom). SANDWICH LEMMA:

   (a) If $H \leq G$ groups and $G \cong \mathbb{Z}^a$ some $a \geq 0$, then $H \cong \mathbb{Z}^b$ some $b \leq a$ [prf: G/H fg ab grp so $G/H \cong \mathbb{Z}^b \oplus A$, A fin ab group, choose $p \nmid |A|$ prime, so $f : G/H \to G/H, x + H \mapsto px + H$ is inj, so can check $f' : H/pH \to G/pG, x + pH \mapsto x + pG$ is inj, so by classification $H \cong \mathbb{Z}^b$, and f' inj $\Rightarrow |H/pH| \leq |G/pG| \Rightarrow p^b \leq p^a \Rightarrow b \leq a$]

   (b) If $K \leq H \leq G$ groups and $K \cong G \cong \mathbb{Z}^a$ then $H \cong \mathbb{Z}^a$ [apply (i) to $K \leq H$ and $H \leq G$ to get $H \cong \mathbb{Z}^b$ where $a \leq b \leq a$]

   (c) If $H \leq G$ groups and $H \cong G \cong \mathbb{Z}^a$ then G/H is finite [by classification, $G/H \cong \mathbb{Z}^n \oplus A$, as before $f' : H/pH \to G/pG$ inj and so by sizes isom, so $G/(H + pG) \cong (\mathbb{Z}/p\mathbb{Z})^n$]

5. $\exists$ int basis for $\mathcal{O}_L$ (use sandwich). disc of L is disc of any int basis. Prop: $L = \mathbb{Q}(\alpha)$, $f(x) \in \mathbb{Q}[x]$ min poly, then $disc(1, \alpha, \alpha^2, .., \alpha^n) = \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{n(n-1)/2}\,\mathrm{N}_{L/\mathbb{Q}}(f'(\alpha))$, proof uses vandermonde. use to compute disc of quad fields:

   (a) $d \equiv 2, 3(\mathrm{mod} 4)$ squarefree $\Rightarrow f(x) = x^2 - d, D_L = 4d$

   (b) $d \equiv 1(\mathrm{mod} 4)$ squarefree $\Rightarrow f(x) = x^2 - x + (1 - d)/4, D_L = d$

   Show $\alpha_1, .., \alpha_{\mathrm{n}} \in \mathcal{O}_L$ and $\mathrm{disc}(\alpha_1, .., \alpha_{\mathrm{n}}) \neq 0$ sqfree integer$\Rightarrow$ $(\alpha_1, .., \alpha_{\mathrm{n}})$ int basis. Port defns to ideals: defn/$\exists$ int basis of ideal, $\mathrm{N}(I) = |\mathcal{O}_L : I|$. Show $\mathrm{disc}(I) = \mathrm{N}(I)^2\,\mathrm{disc}(\mathcal{O}_L)$!!! (prf: smith normal form)

6. $\mathrm{N}((\alpha)) = \left|\mathrm{N}_{L/\mathbb{Q}}(\alpha)\right|$ (follows from last result). START ON IDEALS FORM UFD. def $I + J = (i_l, .., i_n, j_1, .., j_m) = \gcd(I, J)$, $IJ = (i_1j_1, i_1j_2, .., i_nj_m) = \mathrm{lcm}(I, J)$, P prime ideal. show $IJ \subset P \Rightarrow I \subset P$ or $J \subset P$, prime ideals maximal, $I \neq 0$ contains product of prime ideals. $I \subsetneq \mathcal{O}_L \Rightarrow \exists \gamma \in L \setminus \mathcal{O}_L$ st $\gamma I \subset \mathcal{O}_L$.

7. $\forall I, \exists J$ st IJ principal. $IJ = IK \Rightarrow I = J$. $I|J$ iff $I \supset J$ (NB order reversing). $\exists!$ prime factorisation $I = P_1, .., P_n$ (same strt as usual, $\exists$ take min norm counterexample, ! strip factors). Def Ideal Class Group $\mathrm{Cl}(\mathcal{O}_L)$ ideals, equiv if $I = \alpha J$ some $\alpha \in L^*$. Show $\mathcal{O}_L$ PID iff $\mathcal{O}_L$ UFD iff $\mathrm{Cl}(\mathcal{O}_L)$ trivial. Show $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$ (CRT and sheet 2 lemma).

8. DEDEKIND'S CRITERION. First, def if p ramifies/is inert/splits completely. Dedekind's thm: given alg int α st $L = \mathbb{Q}(\alpha)$, min poly $f_\alpha \in \mathbb{Z}[x]$, $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. To prime factor $(p) \subset \mathcal{O}_L$, factor $\bar{f_\alpha} = \prod \bar{g_i}^{e_i}$ over $\mathbb{F}_p$, choose g_i that reduce to $\bar{g_i}$ over $\mathbb{F}_p$, define $Q_i = (p, g_i(\alpha))$. Then $(p) = \prod Q_i^{e_i}$. Example: factor $(5) \subset \mathcal{O}_L$ for $L = \mathbb{Q}(\sqrt{-11})$. $-11 \equiv 1 \bmod 4$ so $\mathcal{O}_L = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})]$, contains $\mathbb{Z}[\sqrt{-11}]$ with index 2, coprime to 5 so reduce $f_\alpha = x^2 + 11 \equiv x^2 + 1 \equiv (x-2)(x-3) \bmod 5$, so $(5) = (5, \sqrt{-11} - 2)(5, \sqrt{-11} - 3)$.

9. Use Ded criterion to factor (p) in quad fields. Start THE GEOMETRY OF NUMBERS. Def a lattice Λ in an f.d. $\mathbb{R}$-vsp V as the $\mathbb{Z}$-span of a basis. Def the covolume $A(\Lambda)$ of lattice as volume of fund. parallelotope. Show $I \subset \mathcal{O}_L$ has $A(\sigma(I)) = \frac{1}{2}\sqrt{|\operatorname{disc}(I)|} = \frac{\mathrm{N}(I)}{2}\sqrt{|D_L|}$. State 2-d Minkowski's thm (used for imaginary quad fields): can find $\lambda \in \Lambda \setminus \{0\}$ st $|\lambda|^2 \leq \frac{4}{\pi}A(\Lambda)$, cor: let $C_L = \frac{2}{\pi}\sqrt{|D_L|}$, then for each $I \neq 0$ can find $\alpha \in I$ non-zero st $\mathrm{N}(\alpha) \leq C_L N(I)$. Cor: for each class $[I] \in \mathrm{Cl}(\mathcal{O}_L), \exists J \in [I]$ st $\mathrm{N}(J) \leq C_L$. All for Thm: $|\mathrm{Cl}(\mathcal{O}_L)| < \infty$, and is generated by prime ideals of norm $\mathrm{N}(P) \leq C_L$(prf uses lagrange). Example: $L = \mathbb{Q}(\sqrt{-7})$. Then $|D_L| = 7$, so $C_L = 2\sqrt{7}/\pi < 2$. No primes $p < 2$ so $\mathrm{Cl}(\mathcal{O}_L)$ trivial so $\mathbb{Q}(\sqrt{-7})$ is a UFD.

10. Generalise Minkowski to n-diml case. Get analogous results, and then useful: $C_L = \left(\frac{4}{\pi}\right)^2 \frac{n!}{n^n}\sqrt{|D_L|}$ is st for any $I \subset \mathcal{O}_L$, can find $\alpha \in I$ st $\mathrm{N}(\alpha) \leq C_l\,\mathrm{N}(I)$. Could cut yourself of this bound.

11. Examples using this bound to compute ideal class group. DIRICHLET'S UNIT THM: Let $\mu_L \subset \mathcal{O}_L^\times$ be group of roots of unity in $\mathcal{O}_L^\times$. Then μ_L is a finite cyclic group and there is an isom $\mathcal{O}_L^\times \cong \mu_L \times \mathbb{Z}^{r+s-1}$. Moreover, this is given by log map with finite kernel μ_L and image $\mathbb{Z}^{r+s-1}$. Use this to find for $r = 2, s = 0$ real quad fields, have $\mathcal{O}_L^\times = \{\pm\alpha^n : n \in Z\}$ ie $\exists$ fund unit.

12. How to find fund unit? First lemma: units in quad fields $u = a + b\sqrt{d}$ or $u = \frac{1}{2}(a + b\sqrt{d})$ (for different cases) with $u > 1$ have $a \geq b \geq 1$. Now to find fund unit: if $d \equiv 2, 3 \bmod 4$ then find min $b \geq 1$ st $db^2 \pm 1$ is square, if $d \equiv 1 \bmod 4$, $d \neq 5$ find min $b \geq 1$ st $db^2 \pm 4$ square, if $d = 5$ do same but pick min such a.

13. Non examble proof of Dirichlet unit thm.

14. Def $\zeta_\mathrm{p} = e^{2\pi i/p}$, pth cyclotomic field $K = \mathbb{Q}(\zeta_\mathrm{p})$. Show $1 - \zeta_\mathrm{p} \in \mathcal{O}_K$ has $\mathrm{N}(1 - \zeta_\mathrm{p}) = p$ and as ideals, $(1 - \zeta_\mathrm{p})^{p-1} = (p)$, and $(1 - \zeta_\mathrm{p})$ is a prime ideal, then that $f_p(x) = (x^p - 1)/(x - 1) \in \mathbb{Z}[x]$ is irred, and $[K : \mathbb{Q}] = p - 1$. $\operatorname{disc}(1, \zeta_\mathrm{p}, .., \zeta_p^{p-2}) = (-1)^{(p-1)/2)}p^{p-2}$ and so $\mathcal{O}_{\mathbb{Q}(\zeta_\mathrm{p})} = \mathbb{Z}[\zeta_\mathrm{p}]$. Useful cor: if l prime ramifies in K then $l = p$.

15. Roots of unity in $\mathbb{Q}(\zeta_\mathrm{p})$ are $\pm\zeta_\mathrm{p}{}^a$ for $a = 0, .., p-1$. Kummer's lemma (examined last year): $u \in \mathcal{O}_k^\times$. Then $\exists a \in \mathbb{Z}$ st $\zeta_p^a u \in K \cap \mathbb{R}$ (hence $[K : K \cap \mathbb{R}] = 2$, in fact $K \cap \mathbb{R} = \mathbb{Q}(\zeta_\mathrm{p} + \zeta_p^{-1})$). Also show $\forall \alpha \in \mathbb{Z}[\zeta_\mathrm{p}]$, $\exists a \in \mathbb{Z}$ st $\alpha^p \equiv a \bmod p$.

16. Non examble