0.1 Fields

Definition 0.1.1. A **division ring** R is a nonzero ring such that $\mathbb{F}^\times = \mathbb{F} - \{0\}$
A **field** $\mathbb{F}$ is a nonzero commutative ring such that $\mathbb{F}^\times = \mathbb{F} - \{0\}$

Definition 0.1.2. A **character** is of G is a group homomorphism $G \to \mathbb{F}^\times$, and a **cocharacter** is a group homomorphism $\mathbb{F}^\times \to G$

Lemma 0.1.3. Characters of G, denoted as $ch(G)$ are linear independent on $\mathbb{F}[G]$

Proof. Suppose not, we can find $c_1\chi_1 + \cdots + c_m\chi_m = 0, c_i \in \mathbb{F}^\times$, with minimal terms, since $\chi_1 \neq \chi_m$, there exists $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_m(g_0)$, on the other hand we have $0 = c_1\chi_1(g) + \cdots + c_m\chi_m(g) = c_1\chi_1(g)\chi_m(g_0) + \cdots + c_m\chi_m(g)\chi_m(g_0), \forall g \in G$ and $0 = c_1\chi_1(gg_0) + \cdots + c_m\chi_m(gg_0) = c_1\chi_1(g)\chi_1(g_0) + \cdots + c_m\chi_m(g)\chi_m(g_0), \forall g \in G$, subtract to get $0 = c_1(\chi_m(g_0) - \chi_1(g_0))\chi_1(g) + \cdots + c_{m-1}(\chi_m(g_0) - \chi_{m-1}(g_0))\chi_{m-1}(g)$ with fewer terms which is a contradiction ☐

Definition 0.1.4. E/F is a field extension, $\alpha \in E$ induces an F-linear automorphism $T_\alpha : E \to E$ by multiplication, then the *field trace* is $\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}\, T_\alpha$. The *field norm* is $N_{E/F}(\alpha) = \det T_\alpha$. Suppose

$$f(x) = \prod(x - \sigma_i(\alpha)) = x^n + a_1x^{n-1} + \cdots + a_n$$

is the minimal monic polynomial, use $1, \alpha, \cdots, \alpha^{n-1}$ as a basis for $F(\alpha)$, then T_α has the matrix form

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ & 1 & \cdots & 0 & -a_{n-2} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & -a_1 \end{bmatrix}$$

Hence $\mathrm{Tr}_{F(\alpha)/F}(\alpha) = -a_1 = \sum \sigma_i(\alpha)$, $N_{F(\alpha)/F}(\alpha) = (-1)^n a_n = \prod \sigma_i(\alpha)$

Definition 0.1.5. $\mathbb{F}$ is a **perfect field** if $\mathbb{F}^p = \mathbb{F}$ if $\mathrm{char}\mathbb{F} = p \neq 0$ or $\mathrm{char}\mathbb{F} = 0$

Definition 0.1.6. E/F is a field extension, $\alpha \in E$ is algebraic over F if α is a zero of some polynomial in $F[x]$. The **algebraic closure** of F in E are the algebraic elements of E

Theorem 0.1.7 (Emil Artin)**.** Any field F has an algebraically closed extension

0.2 Number field

Lemma 0.2.1. $K = \mathbb{Q}[\alpha]$ is number field, f is the minimal polynomial of α. Suppose $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding, then $\sigma(\alpha)$ is a root of f, and any such choice gives an embedding

Definition 0.2.2. E, F are algebraic number fields of finite degree, E/F is finite separable, A, B are corresponding ring of integers, $\{\beta_1, \cdots, \beta_n\}$ is an integral basis of B over A. The **discriminant** of E/F with respect to $\{\beta_1, \cdots, \beta_n\}$ is $D_{E/F}(\beta_1, \cdots, \beta_n) = \det(Tr(\beta_i\beta_j))$

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

Lemma 0.2.3. D_K is well defined in $\dfrac{A}{(A^\times)^2}$

Definition 0.2.4. E, F are algebraic number fields of finite degree, E/F is finite separable, A, B are corresponding ring of integers which are Dedekind domains

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

$pB = q_1^{e_1} \cdots q_r^{e_r}$ with $e_i > 0$. p is **ramified** if $e_i > 1$ for some i, otherwise unramified. p is **inert** if $r = e = 1$. p **totally split** if $e_i = f_i = 1$
$B/pB \cong \prod_{i=1}^r B/q_i^{e_i}$, $f_i = [k_{q_i} : k_p]$, $[E : F] = \dim_{k_p}(B/pB) = \sum_{i=1}^r e_i f_i$
If E/F is Galois, $G = Aut(E/F)$ acts transitively on $\{q_1, \cdots, q_r\}$, then $n = \sum_{i=1}^r e_i f_i = ref$

Proof. $B \cong A^n$, $B/pB \cong A^n/pA^n \cong (A/p)^n \cong k_p^n$ □

Example 0.2.5. $2\mathbb{Z}[i] = (1+i)^2$ is ramified, $3\mathbb{Z}[i]$ is inert, $5\mathbb{Z}[i] = (2+i)(2-i)$ totally split

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[r, hook] & \mathbb{Q}[i] \\ \mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

Theorem 0.2.6. p ramifies in $O_K \Leftrightarrow p \mid \mathrm{disc}(O_K/\mathbb{Z})$

$$\begin{tikzcd} O_K \arrow[r, hook] & K \\ \mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

Proof. $pO_K = \beta_1^{e_1} \cdots \beta_r^{e_r}$, $O_K/pO_K \cong O_K/\beta_i^{e_i}$ is an isomorphism of $\mathbb{F}_p$ algebras. $d_i = \mathrm{disc}((O_K/\beta_i^{e_i})/\mathbb{F}_p))$, $d = \mathrm{disc}((O_K/pO_K)/\mathbb{F}_p))$, thus $d = d_1 \cdots d_r$, since discriminant is functorial, $D = \det(Tr_{O_K/\mathbb{Z}}()) \mapsto d$, $p|D \Leftrightarrow d = 0 \Leftrightarrow d_i = 0$ for some i □