Number Fields

January 25, 2018

Contents

-1 Miscellaneous

Book: Number Fields, Marcus

Course notes: www.dpmms.ac.uk/ jat58/nfl2018

0 Motivation

Theorem. If p is an odd prime, then $p = a^2 + b^2$ for $a, b \in \mathbb{Z} \iff p \equiv 1 \pmod 4$.

Proof. If $p = a^2 + b^2$, then $p \equiv 0, 1, 2 \pmod 4$. So this condition on p is necessary.
Suppose instead $p \equiv 1 \pmod 4$. Then $\left(\frac{-1}{p}\right) = 1$. Thus $\exists a \in \mathbb{Z}$ such that $a^2 \equiv -1 \pmod p$, or $p|a^2 + 1$. We can factor $a^2 + 1 = (a + i)(a - i)$ in the ring $\mathbb{Z}[i]$. Here we introduce a notation: if $R \subseteq S$ are rings and $\alpha \in S$, then

$$R[\alpha] = \{\sum_{i=0}^{n} a_i \alpha^i \in S | a_i \in R\}$$

, the smallest subring of S containing both R and α.

We know from IB GRM that $\mathbb{Z}[i]$ is a UFD. Now $p|(a+i)(a-i)$. If p is irreducible in $\mathbb{Z}[i]$ then $p|a + i$ or $p|a - i$, contradiction. Thus p is reducible in $\mathbb{Z}[i]$, hence $p = z_1 z_2$ with $z_1, z_2 \in \mathbb{Z}[i]$. If $z_1 = A + Bi$, $A, B \in \mathbb{Z}$, then $A^2 + B^2 = p$. $\square$

Another example is when p is an odd prime. Does the equation

$$x^p + y^p = z^p$$

have solutions with $x, y, z \in \mathbb{Z}$ and $xyz \neq 0$?

Theorem. (Kummer, 1850)
If $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD, then there are no solutions.
Strategy: factor $x^p + y^p = \prod_{j=0}^{p-1}(x + e^{2\pi i j/p} y)$ in $\mathbb{Z}[e^{2\pi i/p}]$.

However, we now know $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD $\iff p \leq 19$.

Theorem. (Kummer, 1850)
If p is a *regular* prime, then there are no solutions.
If $p < 100$, then p is regular $\iff p \neq 37, 59, 67$.

We have seen various examples such as $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$, $\mathbb{Z}[e^{2\pi i/p}] \subseteq \mathbb{Q}[e^{2\pi i/p}]$, or in general, $\mathcal{O}_L \subseteq L$, where a ring of "integers" lies in a number field.

1 Ring of integers

Recall: A field extension L/K is an inclusion $K \leq L$ of fields. The degree of L/K is $[L:K] = \dim_K L$. We say L/K is finite if $[L:K] < \infty$.

Definition. (1.1)
A number field is a finite extension $L/\mathbb{Q}$. Here are two ways to construct number fields:
(1) Let $\alpha \in \mathbb{C}$ be an algebraic number. Then $L = \mathbb{Q}(\alpha)$ is a number field;
(2) Let K be a number field, and let $f(X) \in K[X]$ be an irreducible polynomial. Then $L = K[X]/(f(X))$ is a number field.
(Recall Tower Law: $[L:Q] = [L:K][K:Q] < \infty$).

Definition. (1.2)
(1) Let L/K be a field extension. Then we say $\alpha \in L$ is algebraic over K if there exists a monic $f(X) \in K[X]$ such that $f(\alpha) = 0$;
(2) Let $L/\mathbb{Q}$ be a field extension. Then we say $\alpha \in L$ is an algebraic integer if there exists a monic $f(X) \in Z[X]$ such that $f(\alpha) = 0$.

Definition. (1.3)
Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. We call the minimal polynomial of α over K the monic polynomial $f_\alpha(X) \in K[X]$ of least degree such that $f_\alpha(\alpha) = 0$.

We recall why $f_\alpha(X)$ is well-defined: there exists some monic $f(X) \in K[X]$ with $f(\alpha) = 0$ as α is algebraic. If $f_\alpha(\alpha), f'_\alpha(\alpha) \in K[X]$ both satisfy the definition of minimal polynomial, then we apply the polynomial division algorithm to write

$$f_\alpha(X) = p(X)f'_\alpha(X) + r(X)$$

where $p(X), r(X) \in K[X]$, and $\deg r < \deg f'_\alpha$. Evaluate at $X = \alpha$, we have $0 = f_\alpha(\alpha) = p(\alpha)f'_\alpha(\alpha) + r(\alpha) = r(\alpha)$. By minimality of $\deg f'_\alpha$, we must have $r = 0$. Then $\deg f_\alpha = \deg f'_\alpha$, and $f_\alpha(X), f'(\alpha)$ are both monic, i.e. $p(X) = 1$ and $f_\alpha(X) = f'_\alpha(X)$.

Lemma. (1.4)
Let $L/\mathbb{Q}$ be a field extension, and let $\alpha \in L$ be an algebraic integer. Then:
(1) The minimal polynomial $f_\alpha(X)$ of α over $\mathbb{Q}$ lies in $\mathbb{Z}[X]$;
(2) If $g(X) \in \mathbb{Z}[X]$ satisfies $g(\alpha) = 0$, then there exists $q(X) \in \mathbb{Z}[X]$ such that $g(X) = f_\alpha(X)q(X)$;
(3) The kernel of the ring homomorphism $\mathbb{Z}[X] \to L$ by $f(X) \to f(\alpha)$ equals $(f_\alpha(X))$, the ideal generated by $f_\alpha(X)$.

Proof. (1) Recall that if $f(X) = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$, then we define from GRM, the content $c(f) = \gcd(a_n, ..., a_0)$. Recall Gauss' Lemma: If $f(X), g(X) \in \mathbb{Z}[X]$, then $c(fg) = c(f)c(g)$. Since $\alpha \in L$ is an algebraic integer, there exists monic $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$, i.e. $c(f) = 1$. Apply polynomial division in $\mathbb{Q}[X]$ to get $f(X) = p(X)f_\alpha(X) + r(X)$, where $p(X), r(X) \in \mathbb{Q}[X]$, $\deg r < \deg f_\alpha$. The definition of $f_\alpha(X)$ implies that $r(X) = 0$, hence $f(X) = p(X)f_\alpha(X)$. Now choose integers $n, m \geq 1$ such that $np(X) \in \mathbb{Z}[X]$, $c(np) = 1$, and $mf_\alpha(X) \in$

$\mathbb{Z}[x]$, $c(mf_\alpha) = 1$. Then $nmf(x) = (np(x))(mf_\alpha(x)) \implies c(nmf(x)) = nm = 1$. So $n = m = 1$, hence $f_\alpha(x) \in \mathbb{Z}[X]$.
(2) Let $g(X) \in \mathbb{Z}[X]$ be such that $g(\alpha) = 0$. WLOG $g(x) \neq 0$ and $c(g) = 1$. Now apply polynomial division to write $g(x) = q(x)f_\alpha(x) + s(x)$ where $q(x), s(x) \in \mathbb{Q}[x]$, $\deg s < \deg f_\alpha$. Again by definition we have $s(x) = 0$. Choose an integer $k \geq 1$ such that $kq(x) \in Z[x]$ and $c(kq) = 1$. Then $kg(x) = kq(x)f_\alpha(x) \implies k = c(kg) = c(kq)c(f_\alpha) = 1$. So $k = 1$, hence $q(x) \in \mathbb{Z}[x]$.
(3) is a reformulation of (2). □

Let $L/\mathbb{Q}$ be a field extension. Last time we said $\alpha \in L$ is an algebraic integer if $\exists$ monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. We proved that if $\alpha \in L$ is an algebraic integer and $f_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$, then $f_\alpha(x) \in \mathbb{Z}[x]$. However there is a small problem, so we'll prove again.

Proof. Choose $f(x) \in \mathbb{Z}[x]$ monic with $f(\alpha) = 0$, and write

$$f(x) = q(x)f_\alpha(x) + r(x)$$

where $q(x), r(x) \in \mathbb{Q}[x]$, $\deg r < \deg f_\alpha$. Then $r(\alpha) = 0 \implies r(x) = 0$, by minimality of $\deg f_\alpha$. I said that we can find integer $n, m \geq 1$ s.t. $nf\alpha(x) \in \mathbb{Z}[x]$, $c(nf\alpha) = 1$, $mq(x) \in \mathbb{Z}[x]$, $c(mq) = 1$. However we need to explain why do they exist. Note $f_\alpha(x)$ and $q(x)$ are both monic. Choose integers $N, M \geq 1$ such that $Nf_\alpha(x) \in \mathbb{Z}[x]$, $Mq(x) \in \mathbb{Z}[x]$. Then $c(Nf_\alpha)|N$, $c(Mq)|M$ as those are the leading term of the polynomial. Now let $N/c(Nf\alpha) = n \in \mathbb{Z}$, $M/c(Mq) = m \in \mathbb{Z}$. Now $nmf(x) = (nf\alpha(x))(mq(x))$, so $c(nmf(x)) = nm = 1 \implies n = m = 1$. □

Corollary. (1.5)
If $\alpha \in \mathbb{Q}$, then α is an algebraic integer $\iff \alpha \in \mathbb{Z}$.

Proof. By lemma 1.4, α is an algebraic integer $\iff f_\alpha(x) \in \mathbb{Z}[x]$. But if $\alpha \in \mathbb{Q}$, then $f_\alpha(x) = x - \alpha$, and the first needs to divide the second polynomial. □

Notation. If $L/\mathbb{Q}$ is any field extension, we write $\mathcal{O}_L = \{\alpha \in L | \alpha \text{ is an algebraic integer}\}$.

Now we proceed to the first non-trivial result of the course:

Proposition. (1.6)
If $L/\mathbb{Q}$ is a field extension, $\mathcal{O}_L$ is a ring.

Proof. Clearly $0, 1 \in \mathcal{O}_L$. Now if $\alpha \in \mathcal{O}_L$, then $f_{-\alpha}(x) = (-1)^{\deg f_\alpha} f_\alpha(-x) \implies -\alpha \in \mathcal{O}_L$.
The hard part is to show that if $\alpha, \beta \in \mathcal{O}_L$, then $\alpha + \beta \in \mathcal{O}_L$ and $\alpha\beta \in \mathcal{O}_L$.
Observe that if $\alpha \in \mathcal{O}_L$, then $\mathbb{Z}[\alpha] \subseteq L$ is a finitely generated $\mathbb{Z}$-module. By definition, $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \alpha^2, \alpha^3, ...$ Let $f_\alpha(x) = x^d + a_1x^{d-1} + ... + ad$, $a_i \in \mathbb{Z}$. Then $\alpha^d = -(a_1\alpha^{d-1} + ... + ad)$, so $\alpha^d \in \sum_{i=0}^{d-1} \mathbb{Z}\alpha^i$. By induction, we see that $\alpha^n \in \sum_{i=0}^{d-1} \mathbb{Z}\alpha^i$ for all $n \geq d$. Hence $\mathbb{Z}[\alpha] = \sum_{i=0}^{d-1} \mathbb{Z}\alpha^i$. Now take $\alpha, \beta \in \mathcal{O}_L$ and let $d = \deg f_\alpha$, $e = \deg f_\beta$.

By definition, $\mathbb{Z}[\alpha,\beta] = \mathbb{Z}[\alpha][\beta]$ is generated as a $\mathbb{Z}$-module by $\{\alpha^i\beta^j\}_{i,j\in\mathbb{N}}$. The same argument show that in fact this ring is generated as a $\mathbb{Z}$-module by $\{\alpha^i\beta^j\}$ for $0 \le i \le d-1, 0 \le j \le e-1$. So $\mathbb{Z}[\alpha,\beta]$ is finitely generated. From GRM we know the classification of finitely generated $\mathbb{Z}$-modules implies that there's an isomorphism $\mathbb{Z}[\alpha,\beta] \cong \mathbb{Z}^r \oplus T$ for some $r \ge 1$ and finite abelian group T. In fact, $T = 0$: if $\gamma \in T$, then $|T|\gamma = 0$, by Lagrange's theorem. But $\mathbb{Z}[\alpha,\beta] \subseteq L$, a $\mathbb{Q}$-vector space, so this forces $\gamma = 0$. Now we can therefore fix an isomorphism $\mathbb{Z}[\alpha,\beta] \cong \mathbb{Z}^r$ ($r \ge 1$. There's an endomorphism $m_{\alpha\beta} : \mathbb{Z}[\alpha,\beta] \to \mathbb{Z}[\alpha,\beta]$ by $\gamma \to \alpha\beta\gamma$ (as a $\mathbb{Z}$-module). $m_{\alpha\beta}$ corredponds to an $r \times r$ matrx $A_{\alpha\beta} \in M_{r\times r}(\mathbb{Z})$. Let $F_{\alpha\beta}(x) = \det(x \cdot 1_r - A_{\alpha\beta}) \in \mathbb{Z}[x]$, a monic polynomial. By the Cayley-Hamilton theorem, $F_{\alpha\beta}(m_{\alpha\beta}) = 0$ as endomorphisms of $\mathbb{Z}[\alpha,\beta]$. Write $F_{\alpha\beta}(x) = x^r + b_1x^{r-1} + ... + b_r$ for $b_i \in \mathbb{Z}$. Thus $m_{\alpha\beta}^r + b_1m_{\alpha\beta}^{r-1} + ... + b_r \cdot 1_r = 0$ as endomorphisms of $\mathbb{Z}[\alpha,\beta]$.
Now the image of 1 is $(\alpha\beta)^r + b_1(\alpha\beta)^{r-1} + ... + b_r = F_{\alpha\beta}(\alpha\beta) = 0$. So $\alpha\beta \in \mathcal{O}_L$. The argument to show $\alpha+\beta \in \mathcal{O}_L$ is identical, replacing $m_{\alpha\beta}$ by $m_{\alpha+\beta} : \mathbb{Z}[\alpha,\beta] \to \mathbb{Z}[\alpha,\beta]$ by $\gamma \to (\alpha+\beta)\gamma$. The detail is omitted here. □

We call $\mathcal{O}_L$ the ring of algebraic integers of L.

Lemma. (1.7)
Let $L/\mathbb{Q}$ be a number field, and let $\alpha \in L$. Then $\exists n \ge 1$ an integer such that $n\alpha \in \mathcal{O}_L$.

Proof. Let $f(x) \in \mathbb{Q}[x]$ be a monic polynomial such that $f(\alpha) = 0$. Then $\exists n \in \mathbb{Z}, n \ge 1$ such that $g(x) = n^{\deg f} f(x/n) \in \mathbb{Z}[x]$ is monic. But then $g(n\alpha) = n^{\deg f} f(\alpha) = 0$. So $n\alpha \in \mathcal{O}_L$. □

2 Complex embeddings

Let L be a number field.

Definition. (2.1)
A *complex embedding* of L is a field homomorphism $\sigma : L \to \mathbb{C}$. Note: in this case, σ is injective, and $\sigma|_{\mathbb{Q}}$ is the usual embedding $\mathbb{Q} \to \mathbb{C}$.

Proposition. (2.2)
Let L/K be an extension of number fields, and let $\sigma_0 : K \to \mathbb{C}$ be a complex embedding. Then there exist exactly $[L : K]$ embeddings $\sigma : L \to \mathbb{C}$ which extends σ_0 ($\sigma|_K = \sigma_0$).

Proof. Induction on $[L : K]$. If $[L : K] = 1$, then $L = K$, so σ_0 determines σ. In general, choose $\alpha \in L - K$ and consider $L/K(\alpha)/K$. By the Tower law, $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ and $[K(\alpha) : K] > 1$. By induction, it's enough to show there are exactly $[K(\alpha) : K]$ embeddings $\sigma : K(\alpha) \to \mathbb{C}$ extending σ_0. Let $f_\alpha(x) \in K[x]$ be the minimal polynomial of α over K. Observe there's an isomorphism $K[x]/(f_\alpha(x)) \to K(\alpha)$ by sending $x \to \alpha$. To give a complex embedding $\sigma : K(\alpha) \to \mathbb{C}$ extending σ_0, it's equivalent to give a root β of $(\sigma_0 f)(x)$ in $\mathbb{C}$ ($\sigma_0 f(x) \in \mathbb{C}[x]$ means apply σ_0 to the coefficients of $f(x)$). Dictionary: $\sigma \to \beta = \sigma(\alpha)$. We have $[K(\alpha) : K] = \deg f_\alpha = \deg \sigma_0 f_\alpha$. It's enough to show $\sigma_0 f_\alpha$ has distinct roots in $\mathbb{C}$. The polynomial $f_\alpha(x) \in K[x]$ is irreducible, so is prime to its derivative $f'_\alpha(x)$ (*char* $K = 0$). So α is separable over K. $\square$