Number Fields

January 18, 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 polynomail $f_\alpha(X)$ 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). $\square$