Part II - Number Fields

Lectured by

Artur Avameri

Lent 2023

Contents

0 Introduction **2**

1 some title idk what to put here yet **2**

0 Introduction

19 Jan 2022, Lecture 1

This is one of the three deep undergraduate courses, the others being Algebraic Geometry and Algebraic Topology. You should take all three if you one day want to be a mathematician.

1 some title idk what to put here yet

Definition 1.1. Recall that for K, L fields, $K \subset L$, we have a **finite extension** if $\dim_K L < \infty$. This dimension is also written as $[L : K]$, is called the degree of the field extension, and is the dimension of L as a K–vector space.

Definition 1.2. A **number field** is a finite extension over $\mathbb{Q}$.

Definition 1.3. For $\mathbb{Q} \subset L$ a number field, $\alpha \in L$ is an **algebraic integer** if $\exists f \in \mathbb{Z}[X]$ monic such that $f(\alpha) = 0$.

We write $\mathcal{O}_L = \{\alpha \in L \mid \alpha \text{ is an algebraic integer}\}$, the "integers of L".

Lemma 1.1. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, i.e. $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Proof. ($\Longleftarrow$): if $\alpha \in \mathbb{Z}$, then $f(x) = x - \alpha$ is a monic polynomial in $\mathbb{Z}[X]$ such that $f(\alpha) = 0$.

($\Longrightarrow$): Let $\alpha \in \mathbb{Q}$ with $\alpha = \frac{r}{s}$ for r, s coprime in $\mathbb{Z}$. Say $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. Clear denominators to get

$$r^n + a_{n-1}r^{n-1}s + \ldots + a_0 s^n = 0.$$

But s divides everything but the first term, so $s \mid r^n$. If $s \neq 1$, then let $p \mid s$ for p a prime, then $p \mid r$, contradicting $\gcd(r, s) = 1$. $\square$

Theorem 1.2. $\mathcal{O}_L$ is a ring, i.e. if $\alpha, \beta \in L$, then $\alpha \pm \beta, \alpha\beta \in L$.

Remark. $\frac{1}{\alpha}$ usually isn't in $\mathcal{O}_L$.

Recall from Galois Theory that for $\alpha, \beta \in L$ and $K \subset L$, if α, β are algebraic over K, then so are $\alpha \pm \beta$ and $\alpha\beta$. So finite extensions imply algebraic.

Definition 1.4. Let $R \subset S$ be rings. Then

(i) $\alpha \in S$ is **integral over** R if there exists a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[X]$ such that $f(\alpha) = 0$.

(ii) S is **integral over** R if all $\alpha \in S$ are integral over R.

(iii) S is **finitely generated over** R (abbreviated to f.g. $/R$) if there exist elements $\alpha_1, \ldots, \alpha_n \in S$ such that any element of S can be written as an R–linear combination $\alpha_1, \ldots, \alpha_n$, i.e. if the map $R^n \to S$ taking $(r_1, \ldots, r_n) \to \sum r_i\alpha_i$ is surjective.

Example 1.1. Say we have a number field arising from the following picture: *picture*

Then $\alpha \in L$ is an algebraic integer $\iff$ α is integral over $\mathbb{Z}$ (this follows by definition), and $\mathcal{O}_L$ is integral over $\mathbb{Z}$ (once we know it is a ring).

Notation: If $\alpha_1, \ldots, \alpha_r \in S$, then write $R[\alpha_1, \ldots, \alpha_r]$ for the subring of S generated by $R, \alpha_1, \ldots, \alpha_r$. This is the image of the polynomial ring $R[x_1, \ldots, x_r] \to S$ given by $x_i \mapsto \alpha_i$.

Proposition 1.3. (i) If $S = R[s]$ with s integral over R, then S is finitely generated over R.

(ii) If $S = R[s_1, \ldots, s_n]$ with each s_i integral over R, then S is finitely generated over R.

Proof. (i) S is spanned by $1, s, s^2, \ldots$ over R. By assumption $\exists a_0, \ldots, a_{n-1} \in R$ such that $s^n = \sum_{i=0}^{n-1} a_i s^i$, so the R–module spanned by $1, \ldots, s^{n-1}$ is stable by multiplication by s, so it contains $s^{n+1}, s^{n+2}, \ldots$, so is S.

(ii) Let $S_i = R[s_1, \ldots, s_{i-1}]$, so $S_{i+1} = S_i[s_{i+1}]$ and s_{i+1} is integral over R, hence integral over S_i. Hence by (i), S_{i+1} is finitely generated over S_i. To finish, we need to show the following fact, which is left as an exercise:

Exercise: For $A \subset B \subset C$, if B is finitely generated over A and C is finitely generated over B, then C is finitely generated over A.

Sketch of proof: Let $b_1, \ldots, b_r$ generate B over A and $c_1, \ldots, c_s$ generated C over B, then $b_i c_j$ generate C over A.

$\square$

Theorem 1.4. S is finitely generated over $R \implies S$ is integral over R.

Proof. Let $\alpha_1, \ldots, \alpha_n$ generate S as an R–module. Since we can always add elements, we may assume $\alpha_1 = 1$. Let $s \in S$. We will consider $m_s : S \to S$ given by $x \mapsto sx$ (multiplication by s). Then $s\alpha_i = \sum b_{ij}\alpha_j$ for some choice of $b_{ij} \in R$. Let $B = (b_{ij})$. By definition, $(sI - B)\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix} \overset{(\dagger)}{=} 0$. Now recall that for any matrix X, $\operatorname{adj}(X)X = \det(X)$.[1] Multiply ($\dagger$) by $\operatorname{adj}(sI - B)$ to get $\det(sI - B)\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix} = 0$. In particular, $\det(sI - B)\alpha_1 = \det(sI - B) = 0$, so if we define $f(t) = \det(tI - B) \in R[t]$ which is a monic polynomial, then $f(s) = 0$, so s is integral over R. $\square$

[1] Recall that $\operatorname{adj}(X)_{ij}$ is the determinant of the matrix we get when removing the i^{th} row and j^{th} column.

Corollary 1.5. If $\mathbb{Q} \subset L$ is a number field, then $\mathcal{O}_L$ is a ring.

Proof. If $\alpha, \beta \in L$ are algebraic integers, then $\mathbb{Z}[\alpha, \beta]$ is finitely generated over $\mathbb{Z}$ by Proposition 1.3, so it is integral over $\mathbb{Z}$ by Theorem 1.4, so as $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, they are algebraic integers as well. $\square$

Corollary 1.6. If $A \subset B \subset C$ are ring extensions with B/A integral and C/B integral, then C/A is integral.

Proof. If $c \in C$, let $f(x) = \sum_{i=0}^N b_i x^i$ be the monic polynomial over $B[x]$ it satisfies. Set $B_0 = A[b_0, \ldots, b_N]$ and $C_0 = B[c]$, then B_0/A is finitely generated as $b_0, \ldots, b_N \in B$ are algebraic over A, C_0 is finitely generated over B_0 as c is integral over B_0, hence C_0 is finitely generated over A, so C is integral over A by Theorem 1.4. $\square$

Remark. C could have had infinitely many generators, for example $C = \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic integer}\}$, which is why we passed to C_0.

Exercise: Show that $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$, the ring of Gaussian integers.

If $K \subset L$ are fields, then recall that the minimal polynomial of $\alpha \in L$ is the monic polynomial $p_\alpha(x) \in K[x]$ of minimal degree such that $p_\alpha(\alpha) = 0$.

Lemma 1.7. If $f(x) \in K[x]$ has $f(\alpha) = 0$, then $p_\alpha \mid f$.

Proof. Euclid implies $f = p_\alpha h + r$ for $r \in K[x]$ with $\deg(r) < \deg(p_\alpha)$. Hence $0 = f(\alpha) = p_\alpha(\alpha)h(\alpha) + r(\alpha) = r(\alpha)$. If $r \neq 0$, then this contradicts minimality of $\deg(p_\alpha)$. $\square$

The converse is obvious, and the lemma implies that p_α is unique.

Proposition 1.8. Let L be a number field. Then $\alpha \in \mathcal{O}_L \iff$ the minimal polynomial $p_\alpha(x) \in \mathbb{Q}[x]$ of α is in $\mathbb{Z}[x]$.

Proof. ($\Longleftarrow$): By definition, since α is integral.

($\Longrightarrow$): Let $\alpha \in \mathcal{O}_L$ with p_α the minimal polynomial. Let $M \supset L$ be a splitting field for p_α, i.e. the field in which $p(x) = \prod_{i=1}^n (x - \alpha_i)$. Let $h(x)$ be a monic polynomial which α satisfies. By Lemma 1.7, $p_\alpha \mid h$, so each $\alpha_i \in M$ is an algebraic integer. But by Theorem 1.4, sums and products of algebraic integers are algebraic integers, so the coefficients of $p(x)$ are algebraic integers. But $p(x) \in \mathbb{Q}[x]$, so its coefficients are rational algebraic integers, hence they are integers. $\square$

Exercise: Deduce the proposition from Lemma 1.7 and Gauss' lemma.

Lemma 1.9. The field of fractions of $\mathcal{O}_L$ is L. We even prove something stronger: if $\alpha \in L$, then $\exists n \in \mathbb{Z}$ such that $n\alpha \in \mathcal{O}_L$.

Proof. Let $\alpha \in L$ and let g be the minimal polynomial of α (which is monic and in $\mathbb{Q}[x]$). Then $\exists n \in \mathbb{Z}, n \neq 0$ such that $ng \in \mathbb{Z}[x]$, so $h(x) = n^{\deg(g)} g\left(\frac{x}{n}\right) \in \mathbb{Z}[x]$ is monic, and this is the minimal polynomial of $n\alpha$, so $n\alpha \in \mathcal{O}_L$. $\square$