III.L. Algebraic number rings

Let $F = \mathbb{Q}[u_1, \dots, u_n]$ be an algebraic field extension of $\mathbb{Q}$, and $\mathcal{O}_F \subset F$ the subset of **algebraic integers** in F, i.e. elements which are roots of monic polynomials with coefficients in $\mathbb{Z}$. We begin this section by making good on a promise from III.E.8, namely showing that $\mathcal{O}_F$ is a ring. One has to be more clever than to attack this directly; try to check directly that $\sqrt[3]{5} + \frac{1+\sqrt{17}}{2} - 3\mathbf{i}$ is an algebraic integer!

Consider an element $\alpha \in F$, with minimal polynomial $m_\alpha \in \mathbb{Q}[x]$. Recall that this is the unique monic generator of $I_\alpha := \ker\{\mathrm{ev}_\alpha : \mathbb{Q}[x] \to F\}$, or equivalently the lowest-degree (nontrivial, monic) polynomial over $\mathbb{Q}$ having α as a root. Here it is crucial that $\mathbb{Q}[x]$ is a PID.

III.L.1. THEOREM. *The following are equivalent:*
(i) $\alpha \in \mathcal{O}_F$
(ii) $m_\alpha \in \mathbb{Z}[x]$
(iii) $\mathbb{Z}[\alpha]$ *is a finitely generated abelian group*
(*i.e.,* $\mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z}$ *for some* $n \in \mathbb{N}$)
(iv) *There exists a nontrivial f.g. abelian subgroup* $G \leq \mathbb{Q}[\alpha]$ *closed under multiplication by* α.

PROOF. We do this "merry-go-round" style:

(i) $\Longrightarrow$ (ii): By definition of $\mathcal{O}_F$, there exists a monic $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. Then $f \in I_\alpha = (m_\alpha) \subset \mathbb{Q}[x] \implies f = m_\alpha g$ for some $g \in \mathbb{Q}[x]$. But now since f and m_α are monic, $f \in \mathbb{Z}[x]$, and $m_\alpha | f$, we have $m_\alpha \in \mathbb{Z}[x]$ by III.K.11.

(ii) $\Longrightarrow$ (iii): Let $n = \deg(m_\alpha)$, so that

$$m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_i \in \mathbb{Z}.$$

Then $m_\alpha(\alpha) = 0 \implies$

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0 \in \langle 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \rangle,$$

where the RHS denotes the additive abelian subgroup of F generated by these elements. Inductively let $m > n$, and assume we know that

$\alpha^k \in \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$ for $k \leq m-1$. Then

$$\alpha^m = \alpha^{m-n} \cdot \alpha^n \in \langle \alpha^{m-n}, \alpha^{m-n+1}, \ldots, \alpha^{m-1} \rangle \leq \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \rangle.$$

Hence $\mathbb{Z}[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$ as a group.

(iii) $\Longrightarrow$ (iv): Take $G = \mathbb{Z}[\alpha]$. Then

$$\alpha G = \alpha \mathbb{Z}[\alpha] = \langle \alpha, \alpha^2, \ldots, \alpha^n \rangle \leq \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle = \mathbb{Z}[\alpha] = G.$$

(iv) $\Longrightarrow$ (i): Let $G = \langle \gamma_1, \ldots, \gamma_r \rangle \leq \mathbb{Q}[\alpha]$ be a finitely generated abelian subgroup. By assumption on G, we can express

$$\alpha \gamma_i = \sum_{j=1}^{r} \mu_{ij} \gamma_j \qquad (i = 1, \ldots, r) \text{ with } \mu_{ij} \in \mathbb{Z}.$$

Rewriting this in matrix form[35] gives

$$\alpha \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_r \end{pmatrix} = \underbrace{\begin{pmatrix} \mu_{11} & \cdots & \mu_{1r} \\ \vdots & \ddots & \vdots \\ \mu_{r1} & \cdots & \mu_{rr} \end{pmatrix}}_{\mu(\alpha)} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_r \end{pmatrix}$$

and we see that α is an eigenvalue of $\mu(\alpha)$, hence a root of the characteristic polynomial $f(x) := \det(xI_r - \mu(\alpha))$. Now simply observe that f is monic and belongs to $\mathbb{Z}[x]$. □

III.L.2. COROLLARY. *$\mathcal{O}_F$ is a subring of F, called the **ring of integers of F** (or simply an **algebraic number ring**).*

PROOF. We need only check closedness of $\mathcal{O}_F$ under addition and multiplication. Let $\alpha, \beta \in \mathcal{O}_F$. Then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, from which it follows that $\mathbb{Z}[\alpha, \beta]$ is also finitely generated. More concretely, if $\mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z}$ and $\mathbb{Z}[\beta] = \mathbb{Z} + \beta\mathbb{Z} + \cdots + \beta^{m-1}\mathbb{Z}$, then $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha][\beta] = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^i \beta^j \mathbb{Z}$. Both $\mathbb{Z}[\alpha + \beta]$ and $\mathbb{Z}[\alpha\beta]$ are additive subgroups of $\mathbb{Z}[\alpha, \beta]$, and so

[35] The vectors here belong to the vector space $\mathbb{Q}[\alpha]^r$ over the field $\mathbb{Q}[\alpha]$, and the result we are using from linear algebra works over any field: given $M\vec{v} = \lambda\vec{v}$, clearly $\vec{v}$ is in the kernel of left-multiplication by $\lambda I_r - M$, which means the columns of the latter are dependent and hence that its determinant is zero.

are themselves finitely generated (cf. II.K.4). By III.L.1, $\alpha + \beta$ and $\alpha\beta$ belong to $\mathcal{O}_F$. □

III.L.3. EXAMPLE. In HW, you'll show that the p^{th} **cyclotomic polynomial** $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible (for p an odd prime). In $\mathbb{C}[x]$, this factors as $\prod_{k=1}^{p-1}(x - \zeta_p^k)$ where $\zeta_p = e^{\frac{2\pi\mathrm{i}}{p}}$. So all powers of ζ_p are algebraic integers, and $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{Q}[\zeta_p]}$. The field $\mathbb{Q}[\zeta_p] \cong \mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \cdots + 1)$ is called the p^{th} **cyclotomic field**.

Given an arbitrary element $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_{\mathbb{Q}[\zeta_p]}$, we know from III.L.1 that the minimal polynomial has integer coefficients. In fact, one can use Galois theory to show that all the a_i must be integers, hence that $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}[\zeta_p]}$. We will prove this next semester, along with the

III.L.4. PROPOSITION (Kummer). *If $u \in \mathbb{Z}[\zeta_p]^*$, then $u/\bar{u}$ is a root of unity.*

I am stating these results now because we will refer to them in an application at the end of the section.

Integral ideals. Now write, given a number field K, $\mathcal{I}(K)$ for its *monoid of integral ideals* (i.e. nonzero ideals $I \subset \mathcal{O}_K$). Slightly changing notation,[36] we write $\mathcal{J}(K)$ for the *fractional ideals* $\mathfrak{a} = \lambda I$ ($\lambda \in K^*$, $I \in \mathcal{I}(K)$). Recall that $\mathfrak{a} \in \mathcal{J}(K)$ is *invertible* iff $\mathfrak{a} \cdot \mathfrak{b} = \mathcal{O}_K$ for some $\mathfrak{b} \in \mathcal{J}(K)$.

We have seen that

(a) factorization into irreducibles is not necessarily unique, and
(b) irreducibles need not be prime

in a non-UFD $\mathcal{O}_K$. As we shall now see, replacing $\{\mathcal{O}_K^*, \mathcal{O}_K, K\}$ by $\{(1), \mathcal{I}(K), \mathcal{J}(K)\}$ makes these problems disappear.

The proof of the next result requires Galois theory if K is a general number field (as it involves introducing discriminants and ideal-norms in general), so we shall assume it. However, I will explain how it follows from what we already know when K is quadratic.

[36] This is instead of writing $\mathcal{J}(\mathcal{O}_K)$.

III.L.5. THEOREM. (i) *Maximal ideals $I \in \mathcal{I}(K)$ are invertible in $\mathcal{J}(K)$.*
(ii) *There exists a homomorphism of monoids $\mathfrak{N}\colon \mathcal{I}(K) \to \mathbb{N}\backslash\{0\}$ strictly respecting inclusions: $I \supseteq J \implies \mathfrak{N}(I) \leq \mathfrak{N}(J)$ with equality iff $I = J$.*
(iii) *Every ideal $I \in \mathcal{I}(K)$ is finitely generated as an abelian group.*

PROOF FOR $K = \mathbb{Q}[\sqrt{d}]$. (i) We proved $\mathcal{J}(K)$ is a group when we used Hurwitz's theorem to show $\frac{1}{\mathfrak{N}(I)}\tilde{I} \cdot I = (1)$.

(ii) We know $\mathfrak{N}(I \cdot J) = \mathfrak{N}(I) \cdot \mathfrak{N}(J)$. Now if $I \supset J$ then $\tilde{I} \supset \tilde{J}$ $\implies$ $I\tilde{I} \supset J\tilde{J}$ $\implies$ $(\mathfrak{N}(I)) \supset (\mathfrak{N}(J))$ $\implies$ $\mathfrak{N}(I) \mid \mathfrak{N}(J)$ (which is in fact *stronger* than $\mathfrak{N}(I) \leq \mathfrak{N}(J)$). If also $\mathfrak{N}(I) = \mathfrak{N}(J) =: m$, then $\tilde{I} \supseteq \tilde{J} \implies$

$$J = (1)J = \tfrac{1}{m} I \tilde{I} J \supseteq \tfrac{1}{m} J \tilde{J} I = (1)I = I$$

hence $I = J$.

(iii) See Fact III.J.15, proved in III.J.17(b). □

III.L.6. REMARK. (a) From (i), it follows that any product of maximal ideals is invertible in $\mathcal{J}(K)$.

(b) In (iii), I is of rank $[K{:}\mathbb{Q}]$ as an abelian group, at least according to unproved assertions in III.J.17.

(c) For any $I \in \mathcal{I}(K)$, the quotient $\mathcal{O}_K/I$ is a finite abelian group. One can define an ideal norm by $\mathfrak{N}(I) := |\mathcal{O}_K/I|$, which agrees with the definition in the quadratic case.

III.L.7. LEMMA. *Given $I, J \in \mathcal{I}(K)$, with $I \supset J$, and I invertible*[37] *in $\mathcal{J}(K)$. Then:*
(i) $I^{-1}J \in \mathcal{I}(K)$;
(ii) $I \mid J$ *in* $\mathcal{I}(K)$; *and*
(iii) $I^{-1}J \supset J$, *with equality iff* $I = \mathcal{O}_K$.

PROOF. (i) $I \supset J \implies \mathcal{O}_K = I^{-1}I \supset I^{-1}J \implies I^{-1}J \in \mathcal{I}(K)$.

(ii) $I \mid I \cdot I^{-1}J = J$.

(iii) $\mathcal{O}_K \supset I \implies (\mathcal{O}_K \cdot)\, I^{-1}J \supset I \cdot I^{-1}J = J$. If $I^{-1}J = J$ then $\alpha J \subset J$ for each $\alpha \in I^{-1}$. Since J is finitely generated, say $= \langle \beta_1, \ldots, \beta_n \rangle$,

[37] This is in fact always true. See III.L.10.

we can write multiplication by α in this basis: $[\alpha]_{\{\beta\}} =: \mu(\alpha)$, with entries in $\mathbb{Z}$. Set $f(\lambda) := det(\lambda I - \mu(\alpha))$, which as before is monic and integral. By Cayley-Hamilton, $0 = f(\mu(\alpha)) = [f(\alpha)]_{\{\beta\}} \implies f(\alpha) = 0 \implies \alpha \in \mathcal{O}_K$. Since $\alpha \in I^{-1}$ was arbitrary, we have $I^{-1} \subset \mathcal{O}_K \implies \mathcal{O}_K = I\,I^{-1} \subset I\mathcal{O}_K = I \implies I = \mathcal{O}_K$. □

III.L.8. REMARK. Note that $\mathcal{I}(K)^*$ — the invertible elements with inverse in $\mathcal{I}(K)$ — is trivial (= $\{\mathcal{O}_K\}$). This is because if both $I, I^{-1} \in \mathcal{I}(K)$ then $I\,I^{-1} = \mathcal{O}_K \supset I = I\mathcal{O}_K \supset I\,I^{-1} \implies I = \mathcal{O}_K$. Hence the natural definition of "irreducible element" $I \in \mathcal{I}(K)$,

$$\text{“}I = I_1 I_2 \implies I_1 \text{ or } I_2 \text{ is invertible in } \mathcal{I}(K)\text{,”}$$

becomes

$$\text{“}I = I_1 I_2 \implies \text{one of } I_1 \text{ and } I_2 \text{ is just } \mathcal{O}_K\text{”}$$

— no factoring at all. As mentioned at the end of §III.J, this is what we will mean by an *irreducible (integral) ideal*.

III.L.9. THEOREM. *Any $J \in \mathcal{I}(K)$ is a product of maximal ideals.*

PROOF. Suppose otherwise, and choose $J \in \mathcal{I}(K)$ a non-product-of-maximals of smallest possible $\mathfrak{N}(J)$. Observe that J non-maximal $\implies \exists\, I \in \mathcal{I}(K)$ such that $\mathcal{O}_K \supsetneq I \supsetneq J \implies \mathfrak{N}(I) < \mathfrak{N}(J)$ by III.L.5(ii). By "minimality" of $\mathfrak{N}(J)$, I must be a product of maximal ideals; according to III.L.6(a), it is then invertible in $\mathcal{J}(K)$.

By III.L.7, since I is invertible and contains J, we must have $I^{-1}J \in \mathcal{I}(K)$, with $I^{-1}J \supsetneq J$ (since $I \neq \mathcal{O}_K$) hence $\mathfrak{N}(I^{-1}J) < \mathfrak{N}(J)$. Again by "minimality" of $\mathfrak{N}(J)$, $I^{-1}J$ must be a product of maximal ideals, which presents $J = I \cdot (I^{-1}J)$ itself as a product of maximals, a contradiction. □

III.L.10. COROLLARY. (i) *Any $I \in \mathcal{I}(K)$ is invertible in $\mathcal{J}(K)$.*
(ii) *$\mathcal{J}(K)$ is a group* (*abelian, of course*).

PROOF. (i) Use III.L.5(i) and III.L.9.
(ii) Given $\mathfrak{a} = \lambda I$, $\mathfrak{a}^{-1} = \lambda^{-1} I^{-1}$ gives an inverse. □

III.L.11. REMARK. The Corollary implies that Lemma III.L.7 doesn't need the invertibility hypothesis on I. So III.L.7(ii) simply reads

$$I \supset J \quad \iff \quad I \mid J\,,$$

that is, "to divide is to contain". This is a different result than III.D.16, but we will call it **Caesar's lemma** as well.

Note in addition that for $I \supset J$, III.L.7 now gives $J' := I^{-1}J \in \mathcal{I}(K)$, so that $J = IJ'$. By multiplicativity of $\mathfrak{N}$, we get $\mathfrak{N}(J) = \mathfrak{N}(I)\mathfrak{N}(J')$ hence $\mathfrak{N}(I) \mid \mathfrak{N}(J)$.

Before stating the next (extremely important) result, recall that *a priori* "$\wp$ is a prime ideal" means

$$\wp \ni ab \quad \Longrightarrow \quad \wp \ni a \text{ or } \wp \ni b. \tag{III.L.12}$$

Suppose that $\wp$ contains IJ but not I, and let $\imath_0 \in I \backslash (I \cap \wp)$. Then $\imath_0 \jmath \in IJ \subset \wp$ $(\forall \jmath \in J)$, hence all $\jmath \in J$ are in $\wp$ by (III.L.12); conclude that $\wp \supset J$. This gives an alternate characterization

$$\wp \supset IJ \quad \Longrightarrow \quad \wp \supset I \text{ or } \wp \supset J \tag{III.L.13}$$

of primality of $\wp$, which is more suitable for the present context.

III.L.14. PROPOSITION. *For $\wp \in \mathcal{I}(K)$ proper ($\wp \subsetneq \mathcal{O}_K$), the following are equivalent:*
(a) *$\wp$ is irreducible (in $\mathcal{I}(K)$: i.e., doesn't factor at all);*
(b) *$\wp$ is a maximal ideal;*
(c) *$\wp$ is a prime ideal; and*
(d) *$\wp$ is a prime element in $\mathcal{I}(K)$ ($\wp \mid IJ \implies \wp \mid I$ or $\wp \mid J$).*

PROOF. (a) $\Longrightarrow$ (b): If $\wp$ is non-maximal, it is a product of (multiple) maximal ideals by III.L.9, and so is not irreducible.

(b) $\Longrightarrow$ (c): If $\wp$ is maximal, then $\mathcal{O}_K/\wp$ is a field hence a domain, and so $\wp$ is a prime ideal.

(c) $\Longrightarrow$ (d): Caesar.

(d) $\Longrightarrow$ (a): Suppose $\wp$ is a prime element of $\mathcal{I}(K)$, and that $\wp = IJ$ $(I, J \in \mathcal{I}(K))$. Then $\wp \mid I$ or $\wp \mid J$, say the former: $I = \wp\mathcal{Q}$ $(\mathcal{Q} \in \mathcal{I}(K))$

$\implies \wp = IJ = \wp\mathscr{Q}J \implies \mathfrak{N}(\wp) = \mathfrak{N}(\wp)\mathfrak{N}(\mathscr{Q})\mathfrak{N}(J)$ in $\mathbb{N}$. So $\mathfrak{N}(\mathscr{Q}) = 1 = \mathfrak{N}(J)$, whence $\mathscr{Q} = \mathcal{O}_K = J$ by III.L.7(iii). So $\wp$ is irreducible. □

Finally we come to the main point:

III.L.15. COROLLARY. *Any ideal $I \in \mathcal{I}(K)$ has a unique factorization* (*up to order*) *into prime ideals* (*hence into primes/irreducibles in $\mathcal{I}(K)$*).

PROOF. Existence of such a factorization follows from III.L.9 and III.L.14, and one can give a direct proof of uniqueness using Caesar and III.L.7. A more intuitive approach is to use [**Jacobson**, Thm. 2.21] extending our results on UFDs to unique factorization monoids. We want to show $\mathcal{I}(K)$ is a UFM, so it suffices to check DCC and PC. For DCC, use the norm $\mathfrak{N}$ and III.L.5(ii); and PC follows immediately from III.L.14. □

Here is a somewhat obvious but useful result:

III.L.16. COROLLARY. *Let $J \in \mathcal{I}(K)$ have prime norm $\mathfrak{N}(J) \in \mathbb{N}$. Then J satisfies the equivalent conditions of III.L.14.*

PROOF. We need only prove that J is maximal. To this end, suppose otherwise and let $J \subsetneq I \subsetneq \mathcal{O}_K$. Then by III.L.5(ii), $\mathfrak{N}(J) > \mathfrak{N}(I) > 1 (= \mathfrak{N}(\mathcal{O}_K))$. But by III.L.7 (cf. Remark III.L.11), we have $\mathfrak{N}(I)|\mathfrak{N}(J)$, a contradiction since $\mathfrak{N}(J)$ is prime. □

The ideal class group. Next, we denote by $\mathcal{PJ}(K) \leq \mathcal{J}(K)$ the subgroup of *principal fractional ideals*, i.e. those of the form $(\lambda) := \lambda\mathcal{O}_K$, for $\lambda \in K^*$, and by

$$\mathscr{C}\ell(K) := \mathcal{J}(K)/\mathcal{PJ}(K)$$

the *ideal class group*.[38]

III.L.17. DEFINITION. The **class number** of K is the order

$$h_K := |\mathscr{C}\ell(K)|$$

[38]As with $\mathcal{J}(K)$, this is a slight change in notation from III.F.16.

of the ideal class group.[39]

III.L.18. THEOREM. *$\mathcal{O}_K$ is a PID $\iff$ $h_K = 1$.*

PROOF. By definition, $\mathcal{O}_K$ is a PID if and only if all integral ideals are principal, which is to say (i) $\mathcal{I}(K) = \mathcal{I}(K) \cap \mathcal{PJ}(K)$. The class number is 1 exactly when (ii) $\mathcal{J}(K) = \mathcal{PJ}(K)$. Clearly (ii) implies (i) by intersecting both sides with $\mathcal{I}(K)$. Moreover, given $\mathfrak{a} \in \mathcal{J}(K)$, we have $\mathfrak{a} = \lambda I$ for some $I \in \mathcal{I}(K)$; if (i) holds, then I is principal, and then so is $\mathfrak{a}$. Hence (i) implies (ii). □

Write $[\mathfrak{a}] := \mathfrak{a} \cdot \mathcal{PJ}(K)$ for the coset (ideal class) of a fractional ideal $\mathfrak{a}$. The identity element is $[\mathcal{O}_K] = [(1)] =: \mathbf{e}$. Here are some (mostly obvious) rules for working in $\mathscr{C}\ell(K)$:

III.L.19. PROPOSITION. *Let $I, J \in \mathcal{J}(K)$.*
(i) $[I] = \mathbf{e} \iff I \in \mathcal{PJ}(K)$ (*I is principal*).
(ii) $[I] = [J] \iff I \cdot \mathcal{PJ}(K) = J \cdot \mathcal{PJ}(K) \iff I = (\lambda)J$ *for some* $\lambda \in K^* \iff (\alpha)I = (\beta)J$ *for some* $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$.
(iii) $[I][J] = [IJ]$ (*multiplication of cosets*).
(iv) $[I]^{-1} = [I^{-1}]$.
(v) $[I]^m = \mathbf{e} \iff I^m$ *is principal.*
(vi) $IJ = (\alpha) \iff [I]^{-1} = [J]$.

PROOF OF (VI). $\mathbf{e} \underset{\text{(i)}}{=} [(\alpha)] = [IJ] \underset{\text{(iii)}}{=} [I][J]$. □

This is all very useful for solving (or showing insoluble) Diophantine equations like $X^2 = Y^3 - 14$, as you will see in Problem Set 10.

III.L.20. THEOREM. *If the ring of integers $\mathcal{O}_K$ of an algebraic number field is a UFD, then it is a PID.*

III.L.21. COROLLARY. *$h_K = 1 \iff \mathcal{O}_K$ PID $\iff \mathcal{O}_K$ UFD.*

[39] This is always finite, a fact which we will not be able to prove (but see III.L.27 for the idea).

PROOF OF III.L.20 FOR $K = \mathbb{Q}[\sqrt{d}]$. Suppose that $\mathcal{O}_K$ is a UFD. To show that it is a PID (every ideal is principal), it will suffice to prove that its prime ideals are principal, since (by III.L.14) every ideal is a product of maximal ideals, and maximal ideals are prime.

So let $\wp \in \mathcal{I}(K)$ be a prime ideal, and write $\mathfrak{N}(\wp) = \prod_i \sigma_i$ for the (unique) decomposition of its norm into irreducibles *in* $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a UFD, these irreducibles σ_i are prime elements of $\mathcal{O}_K$, so that the (σ_i) are prime ideals, and thus irreducible in $\mathcal{I}(K)$ by III.L.14.

By Hurwitz, $\wp\tilde{\wp} = (\mathfrak{N}(\wp)) \implies \wp \mid (\mathfrak{N}(\wp)) = \prod_i(\sigma_i) \implies \wp \mid (\sigma_i)$ for some i (since $\wp \in \mathcal{I}(K)$ is a prime element). By irreducibility of (σ_i), we have $\wp = (\sigma_i)$, so that $\wp$ is principal as desired. □

III.L.22. REMARK. (a) In a non-UFD $\mathcal{O}_K$, the irreducible σ_i need not be prime, and so the (σ_i) need not be irreducible as elements of $\mathcal{I}(K)$. These principal ideals can and do split up into products of (necessarily) *non-principal* prime ideals.

(b) The observation that $\wp \mid (\mathfrak{N}(\wp))$ does generalize to arbitrary number fields; therefore, so does the above proof.

For all this to be useful for number theory, we need to be able to compute class groups, which requires being able to find all the prime ideals and then all the ideals of a given norm. Consider $K = \mathbb{Q}[\sqrt{d}]$:

III.L.23. LEMMA. *Let $\wp \in \mathcal{I}(K)$ be a prime ideal. Then there exists a unique prime $p \in \mathbb{N}$ such that $\wp \mid (p)$. Hence, if $p \neq 2$ then*

$$\wp = \begin{cases} \wp_p \text{ or } \tilde{\wp}_p & \text{if } (\frac{d}{p}) = 0 \text{ or } 1 \\ (p) & \text{if } (\frac{d}{p}) = -1 \end{cases} \tag{III.L.24}$$

where in the first line $\wp_p := (p, m - \sqrt{d})$ (and $\tilde{\wp}_p = (p, m + \sqrt{d})$) are determined from $d \underset{(p)}{\equiv} m^2$.

PROOF. Let $\mathfrak{N}(\wp) = \prod_i p_i^{n_i}$ be a prime factorization in $\mathbb{N}$. As $\wp$ is prime and $\wp \mid (\mathfrak{N}(\wp))$, we must have $\wp \mid (p_i)$ for some $p_i =: p$. So $\mathfrak{N}(\wp) \mid \mathfrak{N}((p)) = p^2$ (for K quadratic) $\implies \mathfrak{N}(\wp) = p$ or p^2.

If $\mathfrak{N}(\wp) = p$, then (by Hurwitz) $\wp\tilde{\wp} = (p)$, whence $\wp = \wp_p$ or $\tilde{\wp}_p$ since $\mathcal{I}(K)$ is a UFM. If $\mathfrak{N}(\wp) = p^2$, then (by III.L.5(ii)) $\wp = (p)$.

For the uniqueness, if $\wp \mid (q)$ for some other prime q, we get $\mathfrak{N}(\wp) = q$ or q^2; hence $q = p$. □

If $p = 2$, the possibilities are a bit more complicated and depend on the congruence class mod 8 (see Problem Set 10).

Continuing to assume K quadratic, we have the

III.L.25. PROPOSITION. *Let $I \in \mathcal{I}(K)$ and suppose*

$$\mathfrak{N}(I) = \prod_i p_i^{\ell_i} \prod_j {}' p_j^{m_j} \prod_k {}'' p_k^{n_k}$$

is a prime factorization (in $\mathbb{N}$) with $(\frac{d}{p_i}) = 1$, $(\frac{d}{'p_j}) = 0$, and $(\frac{d}{''p_k}) = -1$. Then the $\{n_k\}$ are even, and[40]

$$I = \prod_i \wp_i^{a_i} \tilde{\wp}_i^{\ell_i - a_i} \prod_j {}' \wp_j{}^{m_j} \prod_k ({}'' p_k)^{\frac{n_k}{2}}$$

with $0 \le a_i \le \ell_i$.

PROOF. We have $({}'' p_k)$ irreducible, $({}' p_j) = {}' \wp_j^2$, $(p_i) = \wp_i \tilde{\wp}_i$, and $I \mid (\mathfrak{N}(I)) = \prod_i \wp_i^{\ell_i} \tilde{\wp}_i^{\ell_i} \prod_j {}' \wp_j^{2m_j} \prod_k ({}'' p_k)^{n_k}$. By uniqueness of factorization in $\mathcal{I}(K)$, we have $I = \prod_i \wp_i^{a_i} \tilde{\wp}_i^{b_i} \prod_j {}' \wp_j^{c_j} \prod_k ({}'' p_k)^{d_k}$ where $a_i, b_i \le \ell_i$, $c_j \le 2m_j$, $d_k \le n_k$, and $\prod_i p_i^{\ell_i} \prod_j {}' p_j^{m_j} \prod_k {}'' p_k^{n_k} = \mathfrak{N}(I) = \prod_i p_i^{a_i + b_i} \prod_j {}' p_j^{c_j} \prod_k {}'' p_k^{2d_k}$. By uniqueness of factorization in $\mathbb{N}$, $a_i + b_i = \ell_i$, $c_j = m_j$, and $2d_k = n_k$. □

III.L.26. EXAMPLE. Let $K = \mathbb{Q}[\sqrt{-29}]$. I claim that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$ has an ideal of norm 5 and order 3 in $\mathscr{C}\ell(K)$.

Consider the integer prime $p = 5$: since $-29 \underset{(5)}{\equiv} 1^2$, we have $(5) = (5, 1 - \sqrt{-29})(5, 1 + \sqrt{-29}) = \wp_5 \tilde{\wp}_5$; and by the Proposition, $\wp_5, \tilde{\wp}_5$ are the only ideals of norm 5. Pell's equation $a^2 + 29b^2 = 5$ is insoluble, so $\wp_5$ is non-principal and $[\wp_5]$ is nontrivial.

On the other hand, $a^2 + 29b^2 = 125$ has solutions $(\pm 3, \pm 2)$, and so $(\beta) := (3 + 2\sqrt{-29})$ has norm 5^3. This gives $(\beta) \mid (\mathfrak{N}((\beta))) = (5)^3 = \wp_5^3 \tilde{\wp}_5^3 \implies (\beta) = \wp_5^a \tilde{\wp}_5^{3-a}$ for some $a \in \{0, 1, 2, 3\}$.

[40] The notation here means for instance $\tilde{\wp}_i = \tilde{\wp}_{p_i}$ and ${}' \wp_j = \wp_{'p_j}$.

Now $\beta = 5 - 2(1 - \sqrt{-29}) \in \wp_5$, so that (by Caesar) $\wp_5 \mid (\beta)$. If also $\tilde{\wp}_5 \mid (\beta)$, then $(5) = \wp_5\tilde{\wp}_5 \mid (\beta)$ hence $5 \mid 3 + 2\sqrt{-29}$, which is visibly false.[41] So we conclude that $(\beta) = \wp_5^3$, hence that $[\wp_5]^3 = [\wp_5^3] = [(\beta)] = \mathbf{e}$ as claimed. Note also that $[\tilde{\wp}_5] = [\wp_5]^{-1} = [\wp_5]^2$ since $[\wp_5][\tilde{\wp}_5] = [\wp_5\tilde{\wp}_5] = [(5)] = \mathbf{e}$.

III.L.27. REMARK. In order to compute $\mathscr{C}\ell(K)$ completely, one uses the **Minkowski bound**: for each class $\tau \in \mathscr{C}\ell(K)$, there exists a representative $I \in \mathcal{I}(K)$ (i.e. $[I] = \tau$) satisfying

$$\mathfrak{N}(I) \le B_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta_K|},$$

where $n = [K{:}\mathbb{Q}]$ is the degree, r_2 the number of pairs of conjugate complex embeddings, and Δ_K is the *discriminant*.[42] By III.L.25 (and its generalization to arbitrary number fields), it follows that there are only finitely many ideal classes, so that $h_K < \infty$.

Fermat's equation. The foregoing is useful for treating Diophantine equations, which are polynomial equations in one or more variables with integer coefficients, to which integer solutions are sought. A particularly famous example is

$$x^p + y^p = z^p\,, \qquad p = \text{prime} > 3. \tag{III.L.28}$$

Of course, *Fermat's Last Theorem* states that for *any* exponent $n > 2$, the only solutions to $x^n + y^n = z^n$ are the "trivial" ones, with x or $y = 0$. The cases $n = 4$ (Fermat) and 3 (Euler) were proved by Fermat's *method of descent*; and if one has the theorem for some n, one has it for all exponents divisible by n (why?).

As you may know, the proof was ultimately completed by Wiles in 1995, building on decades of work by many people on modularity and Galois representations. What I want to discuss here is Kummer's big advance in the mid-19th Century, which led to the development of ideals.

[41] That is, $\frac{3}{5} + \frac{2}{5}\sqrt{-29}$ does not belong to $\mathbb{Z}[\sqrt{-29}]$.

[42] Say $K = \mathbb{Q}[\sqrt{d}]$. Then $n = 2$; and r_2 is 1 for $d < 0$ and 0 for $d > 0$. The discriminant is $4d$ unless $d \underset{(4)}{\equiv} 1$, in which case it is d.

Suppose there exists a solution to (III.L.28) in relatively prime $x, y, z \in \mathbb{Z}\backslash\{0\}$, none divisible by p.[43] (In fact, x and y must also be coprime; otherwise $m \mid x, y \implies m^p \mid z^p \implies \gcd(m, z) \neq 1$ violates the relative primality of x, y, z.) We will obtain a contradiction by passing to the "cyclotomic" number ring $\mathbb{Z}[\zeta]$, where ζ denotes a primitive p^{th} root of 1, and considering the equation

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = z^p. \tag{III.L.29}$$

We split the argument up into two cases.

Case 1: $\mathbb{Z}[\zeta]$ a UFD. As the p^{th} cyclotomic polynomial

$$(t-\zeta)\cdots(t-\zeta^{p-1}) = \frac{t^p-1}{t-1} = 1 + t + \cdots + t^{p-1}$$

evaluates to p at $t = 1$,

$$(p) \subset (1-\zeta^a) \qquad \text{for each } a = 1, \ldots, p-1.$$

Since it is irreducible over $\mathbb{Q}$, it is the minimal polynomial of ζ, and thus any element of $K := \mathbb{Q}[\zeta]$ has a unique representation as $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$.

Let $\omega \in \mathbb{Z}[\zeta] = \mathcal{O}_K$ be a prime factor of $x + y\zeta$. By unique factorization and (III.L.29), $\omega \mid z$. If ω also divides $x + y\zeta^{a+1}$ (for some $a \in \{1, \ldots, p-1\}$) then it divides the $\mathbb{Z}[\zeta]$-linear combination

$$\zeta^{-1}(x+y\zeta) - \zeta^{-1}(x+y\zeta^{a+1}) = y(1-\zeta^a)$$

hence yp. Now in $\mathbb{Z}$, $\gcd(z, yp) \mid \gcd(z, y)\cdot\gcd(z, p) = 1\cdot 1 = 1$ $\implies zm + ypm = 1$ for some $n, m \in \mathbb{Z} \implies \omega \mid 1 \implies \omega \in \mathbb{Z}[\zeta]^*$, a contradiction. So ω divides no other factor in LHS(III.L.29).

Since ω divides z, $\omega^p \mid z^p$. No ω-factor can divide other factors (of LHS(III.L.29)), so $\omega^p \mid x + y\zeta$. By uniqueness of the decomposition of $x + y\zeta$ into prime factors, and repeating the argument for

[43] There is a case where one of x, y, z *is* divisible by p, which (while more complicated) can be treated by similar methods.

each prime factor, we find that

$$x + y\zeta = u\alpha^p, \qquad \begin{cases} \alpha \in \mathbb{Z}[\zeta] \\ u \in \mathbb{Z}[\zeta]^*. \end{cases}$$

Write $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$.

Now we apply Kummer's result III.L.4 that $u/\bar{u}$ is a root of 1 in $\mathbb{Z}[\zeta]$, i.e. $\pm\zeta^k$ for some k (we may assume $u/\bar{u} = \zeta^k$). Modulo p, in $\mathbb{Z}[\zeta]/(p)$, we have by the "freshman's dream"

$$\alpha^p \equiv a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{(p-2)p} = \sum_{i=0}^{p-2} a_i^p =: a \in \mathbb{Z}_p.$$

Applying complex conjugation (which preserves the integer prime (p)) to $x + y\zeta = u\alpha^p \equiv ua$ gives $x + y\zeta^{-1} \equiv \bar{u}a$ hence

$$\zeta^k(x + y\zeta^{-1}) = \frac{u}{\bar{u}}(x + y\zeta^{-1}) \equiv ua \equiv x + y\zeta \qquad \mod (p).$$

That is, p divides $x + y\zeta - \zeta^k x - \zeta^{k-1}y$ in $\mathbb{Z}[\zeta]$. By uniqueness of the representation of elements of $\mathbb{Z}[\zeta]$, this is impossible unless $k = 1$. So

$$p \mid (x-y) + \zeta(y-x) \quad \Longrightarrow \quad p \mid x - y \quad \Longrightarrow \quad x \underset{(p)}{\equiv} y.$$

Writing $x^p + (-z)^p = (-y)^p$, we obtain similarly $x \underset{(p)}{\equiv} -z$. But then

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \qquad \mod (p)$$

$\Longrightarrow$ $p \mid 3x^p$, a contradiction.

Case 2: $\mathbb{Z}[\zeta]$ *not* a UFD? Well, we aren't going to prove Fermat's Last Theorem for all odd primes, so there must be a catch. But we can still show non-existence of (nontrivial) solutions in some cases, by reinterpreting (III.L.29) as an equation

$$((x+y))\,((x+y\zeta))\cdots\left((x+y\zeta^{p-1})\right) = (z)^p \tag{III.L.30}$$

of ideals in $\mathbb{Z}[\zeta]$. We may further (uniquely!) factor both sides of (III.L.30) into prime ideals. If some prime ideal $\wp \supset ((x+y\zeta))$ (i.e. $\wp \mid ((x+y\zeta))$), then it can't contain/divide any other of the ideals

on LHS(III.L.30). (Otherwise $\wp \supset (z, yp) = \mathbb{Z}[\zeta]$ as before.) Since $\mathcal{I}(K)$ is a UFM, $\wp \mid (z) \implies \wp^p \mid (z)^p \implies \wp^p \mid ((x + y\zeta))$ and so

$$((x + y\zeta)) = I^p, \quad I \text{ not necessarily principal.}$$

Now suppose that p is a **regular prime**: that is,

$$p \nmid h_K \, (= h_{\mathbb{Q}[\zeta_p]}).$$

In this case, if $[I] \neq \mathbf{e} \in \mathscr{C}\ell(K)$, then by Lagrange we would have $[I]^p \neq \mathbf{e} \in \mathscr{C}\ell(K)$, contradicting principality of $((x + y\zeta))$. Therefore I is principal: $I = (\alpha)$ for some $\alpha \in \mathbb{Z}[\zeta]$. So $((x + y\zeta)) = (\alpha^p)$ hence $x + y\zeta = u\alpha^p$ and we proceed as in Case 1.

The first irregular prime is 37. The method described here essentially settles Fermat for any smaller exponent (prime or not). Note how deeply we dug into the ideal structure of $\mathbb{Z}[\zeta]$ to deal with an equation ostensibly in rational integers!