III.J. Greatest common divisors

III.J.1. DEFINITION. Let R be a commutative ring, and $\mathcal{S} \subset R$ a nonempty subset. Then $\gamma \in R$ is a **GCD** of $\mathcal{S}$ if

$$\begin{cases} \text{(i)} \ \ \gamma \mid s \ (\forall s \in \mathcal{S}), \ \text{ and} \\ \text{(ii)} \ \ \delta \mid s \ (\forall s \in \mathcal{S}) \implies \delta \mid \gamma. \end{cases}$$

If 1 is a GCD of $\mathcal{S}$, then $\mathcal{S}$ is **relatively prime**.[28]

III.J.2. REMARKS. (a) In terms of ideals: (i) $\mathcal{S} \subset (\gamma)$; and (ii) $\mathcal{S} \subset (\delta) \implies (\gamma) \subset (\delta)$. If $\mathcal{S}$ is relatively prime, then $\mathcal{S}$ (or $(\mathcal{S})$) is not contained in a proper principal ideal.

(b) If γ, γ' are two GCDs of $\mathcal{S}$, then (a) $\implies (\gamma) = (\gamma') \implies \gamma \sim \gamma'$. That is, if a GCD exists, it is unique up to units.

(c) R PID $\implies (\mathcal{S}) = (\gamma)$ for some $\gamma \in R$, which is clearly a GCD for $\mathcal{S}$, and $\gamma = s_1 r_1 + \cdots + s_n r_n$ for some $s_j \in \mathcal{S}$, $r_j \in R$.

(c′) Conversely to (c), if *every $\mathcal{S} \subset R$ has a GCD of the form $\gamma = \sum_i s_i r_i$*, then we have $(\mathcal{S}) \supset (\gamma) \supset (\mathcal{S}) \implies (\mathcal{S})$ is principal. Since any $I = (I)$, R is then a PID. (As every UFD is not a PID, the italicized property cannot hold for UFDs in general.)

(d) Dually, we have the notion of **least common multiple (LCM)**: ℓ is a LCM of $\mathcal{S}$ if (i) $s \mid \ell$ $(\forall s \in \mathcal{S})$ and (ii) $s \mid \kappa$ $(\forall s \in \mathcal{S}) \implies \ell \mid \kappa$.

(e) For two elements: γ is a GCD of $a, b \in R$ if: (i) $\gamma \mid a$ and $\gamma \mid b$, and (ii) $\delta \mid a, b \implies \delta \mid \gamma$.

Of course, a GCD need not always exist: in $\mathbb{Z}[\sqrt{10}]$, let $a = 3 + 3\sqrt{10}$, $b = 9$. Then $\delta = 3$ and $\delta' = 1 + \sqrt{10}$ both divide a and b properly (i.e. the quotient is not a unit). Moreover, we have $a \nmid b$, $b \nmid a$, $\delta \nmid \delta'$, and $\delta' \nmid \delta$. Were there a GCD γ of a and b, we'd have[29]

[28] As for ideals, a pair of relatively prime elements ($|\mathcal{S}| = 2$) is said to be *coprime*.

[29] We write $\alpha \parallel \beta$ for "α is a proper divisor of β", which is to say that $\alpha \mid \beta$ and $\frac{\beta}{\alpha}$ is not a unit. The reason we'd have (say) $\delta \parallel \gamma$ here is that, were $\frac{\gamma}{\delta}$ a unit, $\delta' \mid \gamma$ would become $\delta' \mid \delta$, which is false.

$\delta', \delta \parallel \gamma \parallel a, b \implies$

$$\mathcal{N}(\delta) = \mathcal{N}(\delta') = 9 \parallel \mathcal{N}(\gamma) \parallel 81 = \mathcal{N}(a) = \mathcal{N}(b) \quad \implies$$

$\mathcal{N}(\gamma) = 27 \implies \gamma = c + d\sqrt{10}$ with $c^2 - 10d^2 = 27 \implies c^2 \underset{(10)}{\equiv} 7$, a contradiction since 7 is not a square mod 10.

But $\mathbb{Z}[\sqrt{10}]$ (as we know) is not a UFD, and in the UFD case the situation changes:

III.J.3. THEOREM. *Any nonempty subset $\mathcal{S}$ of a UFD R has a GCD.*

PROOF. Write $\mathcal{D} := \left\{ r \in R \,\middle|\, r \mid s \,(\forall s \in \mathcal{S}) \right\} \subset R$ for the set of *all* divisors. Clearly $1 \in \mathcal{D} \implies \mathcal{D} \neq \emptyset$. Recalling the length function $\ell(r)$ (= # of irreducible factors in r) for a UFD, $r \in \mathcal{D} \implies \ell(r) \leq \ell(s)$ $(\forall s \in \mathcal{S}) \implies \exists\, \gamma \in \mathcal{D}$ of maximal length $\ell(\gamma)$.

Let $a \in \mathcal{D}$ be arbitrary. We claim that $a \mid \gamma$, which will establish that γ is a GCD of $\mathcal{S}$.

Write $\mathcal{D}'$ for the common divisors of γ and a. Arguing as above, there exists $c \in \mathcal{D}'$ of maximal length $\ell(c)$; and we may write $a = cd$, $\gamma = c\delta$. Clearly *it is enough to show that $d \in R^*$*, since then $c \mid \gamma \implies a \mid \gamma$.

Suppose this is not so — i.e., that $d \notin R^*$, with irreducible factor f. Then $\ell(cf) = \ell(c) + 1$, while $cf \mid a$. By maximality of $\ell(c)$, we must have $cf \nmid \gamma$, hence $f \nmid \delta$.

Now for every $s \in \mathcal{S}$, we have $a, \gamma \mid s \implies cf \mid s = \gamma\xi = c\delta\xi \implies f \mid \delta\xi$. By III.I.12, since R is a UFD and f is irreducible, f is prime. Since $f \nmid \delta$, it follows that $f \mid \xi$, hence $\gamma f \mid s$. Since s was arbitrary, $\gamma f \in \mathcal{D}$. But $\ell(\gamma f) = \ell(\gamma) + 1$, contradicting maximality of $\ell(\gamma)$. □

III.J.4. DEFINITION. R satisfies the **GCD condition (GCDC)** if every pair $a, b \in R$ has a GCD.

When the GCDC holds, we shall write $\gcd(a, b)$ (which is then well-defined up to a unit).

III.J.5. REMARKS. (i) Note that (by III.J.3) UFDs satisfy the GCDC; and (by III.J.2(c)) for a PID we have $(a, b) = (\gcd(a, b))$.

(ii) The GCDC implies the existence of GCDs for all nonempty *finite* subsets $\mathcal{S} \subset R$. [PROOF: given $\mathcal{S} = \{s_1, \dots, s_n\}$, inductively assume that there exists a GCD γ_0 for $\{s_1, \dots, s_{k-1}\}$. Then $\gamma := \gcd(\gamma_0, s_k)$ has $\gamma \mid \gamma_0 \mid s_1, \dots, s_{k-1}$ and $\gamma \mid s_k$. Moreover, if $\gamma' \mid s_1, \dots, s_k$ then $\gamma \mid s_1, \dots, s_{k-1} \implies \gamma' \mid \gamma_0$, which together with $\gamma' \mid s_k$ yields $\gamma' \mid \gamma$.] So "$\gcd(\mathcal{S})$" makes sense.[30]

(iii) If $\gamma_1 = \gcd(\mathcal{S}_1)$, $\gamma_2 = \gcd(\mathcal{S}_2)$ for two nonempty finite subsets, the same argument gives $\gcd(\mathcal{S}_1 \cup \mathcal{S}_2) = \gcd(\gamma_1, \gamma_2)$.

(iv) If $\gamma = \gcd(\mathcal{S})$ (for a finite subset $\mathcal{S} = \{s_1, \dots, s_n\}$) and $r \in R$, then (writing $r\mathcal{S} := \{rs_1, \dots, rs_n\}$) we have $r\gamma = \gcd(r\mathcal{S})$.

III.J.6. PROPOSITION. *Let R be a commutative domain. Then GCDC $\implies$ PC (primeness condition).*

PROOF. Assume GCDC, and let $\pi \in R$ be irreducible; we claim that π is prime. First note that

$$\gcd(\pi, a) \sim \begin{cases} \pi, & \text{if } \pi \mid a \\ 1, & \text{if } \pi \nmid a. \end{cases}$$

Let $\pi \mid \alpha\beta$ and $\pi \nmid \alpha$. We must show $\pi \mid \beta$.

Suppose otherwise: $\pi \nmid \beta$. Then (writing $(\ ,\ )$ for $\gcd(\ ,\ )$)

$$\begin{aligned} 1 &\sim (\pi, \alpha)(\pi, \beta) \sim ((\pi, \alpha)\pi, (\pi, \alpha)\beta) \\ &\sim \Big((\pi^2, \pi\alpha), (\pi\beta, \alpha\beta)\Big) \sim (\pi^2, \pi\alpha, \pi\beta, \alpha\beta) \\ &\sim (\pi(\pi, \alpha, \beta), \alpha\beta) \sim (\pi, \alpha\beta) \sim \pi, \end{aligned}$$

a contradiction since π is not a unit. □

III.J.7. COROLLARY. *Let R be a commutative domain, with GCDC and DCC. Then R is a UFD.*

[30] The reader may wonder about infinite subsets, since their GCDs exist in III.J.3 for UFDs. But the GCDC doesn't imply R is a UFD, and can't handle infinite subsets, *without also assuming the DCC*. For example, if you are feeling adventurous, try to show that if $R \subset \mathbb{C}$ is the ring of all algebraic integers (i.e. roots of monic polynomials, which we will show yield a ring later on), then the GCDC holds, but $S := \{2^q \mid q \in \mathbb{Q},\ q > \sqrt{2}\} \subset R$ has no GCD.

PROOF. Combine III.J.6 and III.I.12. □

This leads to a second proof that PIDs are UFDs, since the GCDC obviously holds for PIDs (cf. III.J.2(c)).

III.J.8. REMARK. In some of the remarks and computations above, we have treated some aspects of GCDs in terms of ideals. Before proceeding, we want to emphasize that when R is not a PID, some caution is warranted.

Consider that we have two notions of coprimality for a, b in a commutative ring R:

(i) The ideals (a), (b) are coprime if $(a) + (b)\,(= (a, b)) = R$
(ii) The elements a, b are coprime if $\gcd(a, b) = 1$.

Clearly (i) $\implies$ (ii). But (ii) doesn't imply (i) in a non-PID, e.g. in the UFD $\mathbb{F}[x, y]$, (x) and (y) *are not* coprime as ideals, but x and y *are* coprime as elements.

So far we have said a lot about the theory of GCDs, and nothing about effectively computing them (when they are not visibly obvious).

III.J.9. EUCLID'S ALGORITHM. In a PID, $\gcd(\alpha, \beta)$ is the principal generator of (α, β), which gives a clue how to find it. If R is Euclidean, this leads to a (very efficient) algorithm. Define q_i and r_i recursively by

$$\begin{aligned} \alpha &= q_1\beta + r_1 && \delta(r_1) < \delta(\beta) \quad [\text{or } r_1 = 0] \\ \beta &= q_2 r_1 + r_2 && \delta(r_2) < \delta(r_1) \quad [\text{or } r_2 = 0] \\ r_1 &= q_3 r_2 + r_3 && \delta(r_3) < \delta(r_2) \quad [\text{or } r_3 = 0] \\ &\vdots && \vdots \end{aligned}$$

As δ doesn't take negative values, eventually some $r_{n+1} = 0$ (where $r_n \neq 0$):

$$r_{n-1} = q_{n+1} r_n + 0.$$

Now look at this in terms of *ideals*:

$$\begin{aligned}(\alpha,\beta) &= (q_1\beta + r_1, \beta) = \\ (\beta, r_1) &= (q_2 r_1 + r_2, r_1) = \\ (r_1, r_2) &= (q_3 r_2 + r_3, r_2) = \\ (r_2, r_3) &= \quad \cdots \quad = \\ (r_{n-1}, r_n) &= (q_{n+1} r_n, r_n) = (r_n).\end{aligned}$$

This proves the

III.J.10. THEOREM. *For α, β in a Euclidean domain R, $\gcd(\alpha,\beta)$ is the last nonzero remainder in the Euclidean algorithm.*

We now turn to a couple of applications of Euclid's algorithm and GCDs in $\mathbb{Z}$.

Application 1: The RSA cryptosystem.

III.J.11. PROPOSITION. *Suppose $k, k', m \in \mathbb{Z}_{>1}$, $\gcd(a,m) = 1$, and $kk' \underset{\phi(m)}{\equiv} 1$. Then $a^{kk'} \underset{(m)}{\equiv} a$.*

PROOF. Since $a \in \mathbb{Z}_m^*$, we have $a^{\phi(m)} \underset{(m)}{\equiv} 1$ by Euler's theorem II.D.9, and so $a^{kk'} = a \cdot a^{N\phi(m)} = a(a^{\phi(m)})^N \underset{(m)}{\equiv} a$. □

As k is invertible mod $\phi(m)$ provided they are coprime, we have

III.J.12. COROLLARY. *The map $(\cdot)^k \colon \mathbb{Z}_m^* \to \mathbb{Z}_m^*$ is an isomorphism if $\gcd(k, \phi(m)) = 1$, and has inverse $(\cdot)^{k'}$.*

Say you want to be able to receive secure communications from me over a public channel:

You Pick two large primes p, q, put $m = pq$. Then $\phi(m) = (p-1)(q-1)$. Now

(III.J.13) $$\boxed{\begin{array}{c}\text{let } k \in (0, \phi(m)) \cap \mathbb{Z} \text{ be large,} \\ \text{with } (k, \phi(m)) = 1, \text{ and find } k'.\end{array}}$$

Make m, k public; and keep $p, q, \phi(m), k'$ secret.

Me I take a message, encode it as a single number $a \in (0, m) \cap \mathbb{Z}$, and send you

$$b := \bar{a}^k \in \mathbb{Z}_m.$$

You Compute $\bar{b}^{k'} \in \mathbb{Z}_m$, recovering (by III.J.11) my message a.

Suppose someone overhears m, k, b and wants to break the code to recover a. They must find k', which requires knowing $\phi(m)$, for which they will need to be able to factor m (into p and q). Unless they have a quantum computer, this could take centuries.

As for us, how do we manage III.J.13? By using Euclid: first, to check $\gcd(k, \phi(m)) = 1$; but less obviously, to solve the congruence $kk' \underset{\phi(m)}{\equiv} 1$:

$$\begin{aligned}
\phi(m) = kq_0 + r_0 \quad &\implies r_0 = \phi(m) - kq_0 \underset{\phi(m)}{\equiv} -kq_0 \\
k = r_0q_1 + r_1 \quad &\implies r_1 = k - r_0q_1 \underset{\phi(m)}{\equiv} k + kq_0q_1 = k(1 + q_0q_1) \\
r_0 = r_1q_2 + r_2 \quad &\implies r_2 = r_0 - r_1q_2 \underset{\phi(m)}{\equiv} -kq_0 - k(1 + q_0q_1)q_2 \\
\vdots \quad &\qquad\qquad = -k(q_0 + q_2 + q_0q_1q_2)
\end{aligned}$$

Eventually, some $r_n = 1$ and so the algorithm gives

$$1 \underset{\phi(m)}{\equiv} k \cdot (\text{big mess}).$$

The big mess is our k'.

Application 2: Prime factorization in quadratic fields. Let p be an *odd* prime number ($\in \mathbb{N}$), and $K = \mathbb{Q}[\sqrt{d}]$ a quadratic number field (d squarefree). Below, (p) will mean $p\mathcal{O}_K$, i.e. the ideal $(p) \subset \mathcal{O}_K$. Denote by $\mathcal{I}(K)$ the **monoid of ideals**[31] in $\mathcal{O}_K$. An element $I \in \mathcal{I}(K)$ is *irreducible* if we cannot write $I = I_1I_2$, with both I_1, I_2 proper in $\mathcal{O}_K$. We would like to factor (p) in $\mathcal{I}(K)$ as a product of irreducibles.

[31] cf. Problem Set 7 #4. Here we take this to consist of all *nonzero* ideals.

We know that $\mathcal{O}_K$ is often not a UFD, and that GCDs may not exist. So we are not going to take them in $\mathcal{O}_K$. Rather, the connection of this section to GCDs comes from Hurwitz's theorem (cf. III.F.17). Recall that given $I = (\alpha, \beta) \subset \mathcal{O}_K$ and $\tilde{I} = (\tilde{\alpha}, \tilde{\beta})$, it says that

- $\alpha\tilde{\alpha}$, $\beta\tilde{\beta}$, and $\alpha\tilde{\beta} + \beta\tilde{\alpha}$ belong to $\mathbb{Z}$, and
- if g is their GCD in $\mathbb{Z}$, then $I\tilde{I} = (g) = g\mathcal{O}_K$.

It is the main tool in the proof of the following

III.J.14. THEOREM. *As an element of $\mathcal{I}(K)$, the ideal $(p) \subset \mathcal{O}_K$ decomposes into irreducibles as follows:*

(i) $d \underset{(p)}{\equiv} 0 \implies (p) = (p, \sqrt{d})^2 =: \wp_p{}^2$, *and we say* ***p ramifies****.*

(ii) $d \underset{(p)}{\equiv} m^2 \underset{(p)}{\not\equiv} 0 \implies (p) = (p, m - \sqrt{d})(p, m + \sqrt{d}) =: \wp_p\tilde{\wp}_p$ (*where* $\wp_p \neq \tilde{\wp}_p$), *and we say* ***p splits****.*

(iii) $d \underset{(p)}{\not\equiv}$ *square* $\implies (p)$ *is irreducible in* $\mathcal{O}_K$, *and we say* ***p is inert****.*

PROOF. Introduce the **ideal norm** $\mathfrak{N}\colon \mathcal{I}(K) \to \mathbb{N}\backslash\{0\}$, sending a nonzero ideal $I \subset \mathcal{O}_K$ to the unique generator in $\mathbb{N}$ of $I\tilde{I}$. (That is, $I\tilde{I} = (\mathfrak{N}(I))$.) This is well-defined by Hurwitz, and is a multiplicative monoid homomorphism. Moreover, it is useful for detecting irreducibles: if $\mathfrak{N}(I) = 1$, then

$$I\tilde{I} = (\mathfrak{N}(I)) = (1) = \mathcal{O}_K \subseteq I = I\mathcal{O}_K \subseteq I\tilde{I}$$

forces $I = \mathcal{O}_K$. So if $\mathfrak{N}(I)$ is prime, then I is irreducible in $\mathcal{I}(K)$.

For (i), combining Hurwitz with the fact that d is squarefree and divisible by p, we get $\wp_p{}^2 = (p, \sqrt{d})(p, \sqrt{d}) = (\gcd_{\mathbb{Z}}(p^2, 0, d)) = (p)$ $\implies \mathfrak{N}(\wp_p) = p \implies pr$ irreducible.

For (ii), again by Hurwitz we have

$$\begin{aligned}\wp_p\tilde{\wp}_p = (p, m - \sqrt{d})(p, m + \sqrt{d}) &= (\gcd_{\mathbb{Z}}(p^2, 2pm, m^2 - d)) \\ &= (p \cdot \gcd_{\mathbb{Z}}(p, 2m, n)) = (p)\end{aligned}$$

since p odd and $m \underset{(p)}{\not\equiv} 0 \implies p, 2m$ coprime. Again $\mathfrak{N}(\wp_p) = p = \mathfrak{N}(\tilde{\wp}_p)$, and so both $\wp_p$ and $\tilde{\wp}_p$ are irreducible.

Finally, for (iii), begin by noting that $\mathfrak{N}((p)) = p^2$, and suppose that (p) is not irreducible. Then there exists an ideal I of norm p with $I \supsetneq (p)$ (as (p) must break into two such). Assume the following

III.J.15. FACT. *Every $I \in \mathcal{I}(K)$ is generated by 2 elements of $\mathcal{O}_K$.*

which will be proved in a moment. Then $I = (\alpha, \beta) \implies p = \gcd_{\mathbb{Z}}(\alpha\tilde{\alpha}, \beta\tilde{\beta}, \alpha\tilde{\beta} + \beta\tilde{\alpha})$. Since $I \supsetneq (p)$, p cannot divide both α and β; say $p \nmid \alpha = \frac{r+s\sqrt{d}}{2}$ (where $r \underset{(2)}{\equiv} s$).

On the other hand, $p \mid \alpha\tilde{\alpha} = \frac{r^2-s^2d}{4} \implies r^2 \underset{(4p)}{\equiv} s^2d$. If $p \mid s$ then $p \mid r$ and so (writing $r = pr'$, $s = ps'$, with $r' \underset{(2)}{\equiv} s'$) we have $\alpha = \frac{pr'+ps'\sqrt{d}}{2} = p(\frac{r'+s'\sqrt{d}}{2})$ hence $p|\alpha$, a contradiction. Therefore $p \nmid s$, and there exists an inverse $s^{-1} \in \mathbb{Z}_p$. We then find that

$$d \underset{(p)}{\equiv} (ss^{-1})^2 d \underset{(p)}{\equiv} s^2 d(s^{-1})^2 \underset{(p)}{\equiv} r^2(s^{-1})^2 \underset{(p)}{\equiv} (rs^{-1})^2,$$

in contradiction to our hypothesis in (iii). Conclude that I cannot exist, and (p) is irreducible. □

Here is a standard bit of notation attached to III.J.14.

III.J.16. DEFINITION. Define the **Legendre symbol** by

$$\left(\frac{d}{p}\right) := \begin{cases} 0 & \text{in case (i)} \\ 1 & \text{in case (ii)} \\ -1 & \text{in case (iii)} \end{cases}$$

It won't be used until a later section.

We now prove Fact III.J.15 — actually a bit more. Recall:

- any subgroup $\mathbb{K} \leq \mathbb{Z}^n$ is $\cong \mathbb{Z}^m$ for some $m \leq n$ (cf. II.K.4); and
- any quadratic number field is of the form $\mathbb{Q}[x]/(x^2 - d)$ (with elements of the form $q_1 + q_2 x$) hence a $\mathbb{Q}$-vector space of dimension 2. In fact, for a general number field F,[32] we'll show in the Galois theory unit that $F \cong \mathbb{Q}[x]/(m_u)$ for some minimal polynomial m_u of degree n, so that $\dim_{\mathbb{Q}} F = n =: [F{:}\mathbb{Q}]$.

[32] We already saw this for number fields of the form $\mathbb{Q}[u]$ (cf. III.G.9 and its proof, and III.H.13); the point here is that even those which appear to require multiple generators really have just one.

III.J.17. PROPOSITION.

(a) Let F be a number field, $\mathcal{O}_F$ its ring of integers.[33]

(i) Every nonzero ideal $I \subset \mathcal{O}_F$ contains a basis for F as a $\mathbb{Q}$-vector space, hence a subgroup $\cong \mathbb{Z}^{[F:\mathbb{Q}]}$.

(ii) Assuming that $\mathcal{O}_F \cong \mathbb{Z}^{[F:\mathbb{Q}]}$ (and $F \cong \mathbb{Q}^{[F:\mathbb{Q}]}$),[34] *we have that $I \cong \mathbb{Z}^{[F:\mathbb{Q}]}$, with basis spanning $F/\mathbb{Q}$.*

(b) Let $K = \mathbb{Q}[\sqrt{d}]$, and $I \subset \mathcal{O}_K$ be a nonzero ideal. Then as an additive abelian group, $I = \langle \gamma, \delta \rangle$, for some $\gamma, \delta \in \mathcal{O}_K$; and, moreover, $I = (\gamma, \delta)$.

PROOF. (a) (i) If $\beta_1, \dots, \beta_n$ ($n = [F:\mathbb{Q}]$) is a basis for $F/\mathbb{Q}$, then I claim that there exists $b \in \mathbb{Z}$ such that $b\beta_i \in \mathcal{O}_F$ ($\forall i$). To see this, note that each β_i satisfies some monic rational polynomial equation, as F is algebraic over $\mathbb{Q}$. Taking b to be the product of all denominators of the coefficients of this equation, the $b\beta_i$ will satisfy equations with integer coefficients:

$$\begin{aligned} & \beta^d + \tfrac{a_1}{b_1}\beta^{d-1} + \tfrac{a_2}{b_2}\beta^{d-2} + \cdots + \tfrac{a_d}{b_d} = 0 \\ \implies \quad & \tfrac{(b\beta)^d}{b^d} + \tfrac{a_1}{b_1 b^{d-1}}(b\beta)^{d-1} + \tfrac{a_2}{b_2 b^{d-2}}(b\beta)^{d-2} + \cdots + \tfrac{a_d}{b_d} = 0 \\ \implies \quad & (b\beta)^d + a_1 \tfrac{b}{b_1}(b\beta)^{d-1} + a_2 \tfrac{b^2}{b_2}(b\beta)^{d-2} + \cdots + a_d \tfrac{b^d}{b_d} = 0. \end{aligned}$$

Next, taking any $\alpha \in I \backslash \{0\}$, each $b\beta_i\alpha \in I$; and since (in F) multiplication by αb is invertible, the $\{b\beta_i\alpha\}$ cannot satisfy a nontrivial $\mathbb{Q}$-linear relation (without contradicting linear independence of the $\{\beta_i\}$). So I contains a $\mathbb{Z}^n$.

(ii) Applying II.K.4 to $I \leq \mathcal{O}_F \cong \mathbb{Z}^n$ gives $I \cong \mathbb{Z}^m$ for some $m \leq n$. Applying it to the result of (i) (that I contains a subgroup isomorphic to $\mathbb{Z}^n$) gives $n \leq m$. So $m = n$.

(b) We have $\mathcal{O}_K \cong \langle 1, \sqrt{d} \rangle$ or $\langle 1, \frac{1+\sqrt{d}}{2} \rangle$, in either case isomorphic to $\mathbb{Z}^2$ as an abelian group. So (a)(ii) yields $I \cong \mathbb{Z}^2$; and writing $I = \langle \gamma, \delta \rangle$ ($\mathbb{Z}$-linear combinations of γ, δ), we clearly have $I \subset (\gamma, \delta)$ ($\mathcal{O}_K$-linear combinations). Since $\gamma, \delta \in I$ and I is an ideal, we also have $I \supset (\gamma, \delta)$. □

[33] We have yet to check that this is a ring, except for $F = \mathbb{Q}[\sqrt{d}]$.

[34] These will turn out to be always true (as we already know for quadratic fields).