

TYPOS TO BE CORRECTED IN THE FOURTH PRINTING OF ANT

PAGE NUMBER	LINE NUMBER	MISPRINT → CORRECTION
3	11	an algebraic integer → $\alpha \in R$
3	15	factorization. → factorization, Thus, for example, a field always has unique factorization.
3	-6 (above footnote)	delete <i>algebraic integer</i>
36	11	Add to the end of the statement of Theorem 1.63: “Moreover, $D \in \mathbb{Z}$ if \mathcal{B}_1 is an integral basis and $\mathcal{B}_2 \in \mathcal{O}_F$.”
83	17	$\alpha_j \rightarrow \alpha_{j-1}$
85	3	$\zeta_{p^a}^{p^a-1}$ is a $(p^a)^{th}$ → $\zeta_{p^a}^{p^a-1}$ is a p^{th}
88	Exercise 2.29	p^{th} root → $p^a - th$ root
108	11	$\alpha_{r_2} \rightarrow \alpha_{r_1+r_2}$ (twice)
149	-4	$2 + \sqrt{10}, 2 - \sqrt{10} \rightarrow 4 + \sqrt{10}, 4 - \sqrt{10}$
235	8	$\mathcal{G}al(K/F) \rightarrow \mathcal{G}al(L/F)$
339	-9	$P + Q + R = 0 \rightarrow P + Q + R = \mathfrak{o}$

Thanks go to Pete Klimek for observing that in the proof of Theorem 1.35 on page 21, in line -4, the root α_j should be of $m_{\alpha, F}^\theta(x)$ rather than $m_{\alpha, F}(x)$

As observed by Don Kreher of Michigan Technological University, in Example 1.27 on page 18, $\alpha_{1,2} = -g$ is incorrect. It should be $\alpha_{1,2} = 1 - g$. Also, he and his students noted the following. On page 59, Equation (1.110) should read:

$$\left(\frac{x + \sqrt{-7}}{2}\right) = \pm \left(\frac{1 \pm \sqrt{-7}}{2}\right)^m.$$

Moreover, after the displayed equation above (1.110), add the following comment:

Note that neither $(1 + \sqrt{-7})/2$ nor $(1 - \sqrt{-7})/2$ is a common factor of the terms on the left since such a factor would divide their sum x , from which it follows that $2|x$, contradicting that x is odd.

On page 60, line -3, the modulus should be $(\text{mod } 7^\ell)$, and lines -8 through -4 on page 60 would better be stated as follows:

An easy iterative argument leads to the congruence

$$\alpha^{m_1-m} \equiv 1 + (m_1 - m)\sqrt{-7} \pmod{7^{\ell+1}}.$$

On page 76, line 9, replace: “which is on the list.” by “but $D \equiv 1 \pmod{4}$, so so $\epsilon = 2$, not 1, a contradiction. Thus, (2.8) cannot hold.”

Thanks go to Professor Carlos Jacob Rubio of the Universidad Autonoma de Yucatan, Mexico for observing a problem with a part of the proof of Theorem 2.1 on page 74. Replace Case 2.4 on page 74 with the following:

CASE 2.4. $D = \Delta_F \equiv 1 \pmod{4}$.

In this case, $\alpha = (a + b\sqrt{D})/2$ for $a, b \in \mathbb{Z}$. Since $\Delta_F \equiv 1 \pmod{4}$ and $\Delta_F < -12$, we have that $\Delta_F \leq -15$. Hence for $\alpha \neq 0, \pm 1$,

$$12 \geq a^2 - b^2 D \geq a^2 + 15b^2 > 15,$$

a contradiction.

He also found a problem with the proof of Theorem 2.5 on page 76. Delete the first 6 lines on page 76 (up to and including $r_1 = 1/2$) and replace by:

$$(r_1 + 1)^2 \geq 1 + r_2^2 D / \epsilon^2 \geq 2 + r_1^2 \tag{2.12}$$

which follows from (1.10), so $r_1 \geq 1/2$. However $r_1 \leq 1/2$ so $r_1 = 1/2$.

He also queried why, on page 83 in the proof of Claim 2.31 of Theorem 2.30’s proof that we may assume p does not divide z_d . To see this, note that there *exists* some β for which this holds so we may assume without loss of generality that this holds. For instance, if $\Delta_F = p^r$ and $\beta = \sum_{j=d}^{\phi(p^a)} z_j \alpha_{j-1}$ where p^r does not divide z_d then merely multiply β by p^{r-1} and replace the original β with this one.

Thank go to Jin Yuan for asking about Exercise 3.15 on page 139. This is incorrect without the assumption that R is a Dedekind domain. and if such is assumed the solution follows from Exercise 3.17. When R is not a Dedekind domain only one direction holds, namely $(I \cap J)(I + J) \subseteq IJ$, and the proof for this holds as given on page 428. However, there is a flaw in the proof of the converse, and indeed here is a counterexample to that converse. Let R be the real field, set $R = \mathbb{R}[x, y]$, the polynomial ring, set $I = \langle x^2 y \rangle$, and $J = \langle xy^2 \rangle$. Then $(I \cap J)(I + J)$ is properly contained in $IJ = \langle x^3 y^3 \rangle$.

As pointed out by Bill Rosgen, one of my ANT graduate students in the winter, 2006 term, there is a typo in Exercise 3.49 on page 151. The second sentence should read: “If $\alpha, \beta \in \mathcal{O}_F, \dots$ ”, NOT “If $\alpha, \beta \in I$ ”

Thanks go to Jacob Rubio for observing that the $a = -1$ value in Example 3.36 on page 145 is unnecessary.

Jose Adrian Rodriguez Fonollosa has pointed out that the solution to Exercise 1.79 on page 414 is incorrect since Equation (S8) is wrong and fails to match the matrix equation below it. He has come up with a solution based on my approach, which is not as lengthy as my version. Here it is:

Let $F = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$, $K = \mathbb{Q}(\sqrt{-14})$, and $\mathfrak{D}_K = \mathbb{Z}[\sqrt{-14}]$.
 If $\mathfrak{D}_F = \mathbb{Z}[\alpha, \sqrt{-14}]$ for some $\alpha \in \mathfrak{D}_F$, then in particular,

$$\Delta = \frac{1 + \sqrt{-7}}{2} = \gamma_1 \alpha + \gamma_2, \text{ where } \Delta \in \mathfrak{D}_F, \gamma_1, \gamma_2 \in \mathfrak{D}_K,$$

and

$$\sqrt{-14}/\sqrt{-7} = \sqrt{2} = \beta_1 \alpha + \beta_2 \text{ where } \sqrt{2} \in \mathfrak{D}_F, \text{ and } \beta_1, \beta_2 \in \mathfrak{D}_K.$$

Let θ be the embedding of F in \mathbb{C} given by,

$$\theta : \sqrt{-7} \mapsto -\sqrt{-7}, \text{ and } \theta : \sqrt{-14} \mapsto \sqrt{-14}.$$

In other words, θ fixes K pointwise. Then we get,

$$\begin{aligned} \theta(\Delta) &= \frac{1 - \sqrt{-7}}{2} = \gamma_1 \theta(\alpha) + \gamma_2, \\ \Delta - \theta(\Delta) &= \sqrt{-7} = \gamma_1(\alpha - \theta(\alpha)) \end{aligned} \tag{1}$$

and

$$\begin{aligned} \theta(\sqrt{2}) &= -\sqrt{2} = \beta_1 \theta(\alpha) + \beta_2, \\ \sqrt{2} - \theta(\sqrt{2}) &= 2\sqrt{2} = \beta_1(\alpha - \theta(\alpha)). \end{aligned} \tag{2}$$

Then squaring equations (??)–(??), and taking norms from K ,

$$7^2 = N_K(\gamma_1)^2 N_K((\alpha - \theta(\alpha))^2), \text{ and } 2^6 = N_K(\beta_1)^2 N_K((\alpha - \theta(\alpha))^2)$$

with $N_K(\gamma_1) \in \mathbb{Z}$, $N_K(\beta_1) \in \mathbb{Z}$, $(\alpha - \theta(\alpha))^2 \in \mathfrak{D}_K$, and $N_K((\alpha - \theta(\alpha))^2) \in \mathbb{Z}$, which is impossible since α is a basis element (and it is readily checked that $\alpha - \theta(\alpha)$ cannot be a unit).

Several people also pointed out that the solution of Exercise 1.115 on page 419 is incomplete. We have to show that $\mathbb{Z}[\alpha]$ not only is a *basis of integers* for F but an *integral basis* for F . This can be fixed as follows.

This can be done by proving that the field and basis discriminants are the same.

Since $|\Delta_F|$ is minimal over all discriminants of bases for F over \mathbb{Q} , then by Theorem 1.63,

$$\text{disc}\{1, \alpha, \alpha^2\} = D^2 \Delta_F,$$

where $D = |\mathcal{O}_F : \mathbb{Z}[\alpha]|$ (see Exercise 2.26 on page 88 as well). Also, we compute that

$$\text{disc}\{1, \alpha, \alpha^2\} = -108 = -2^2 \cdot 3^3.$$

Since

$$|\mathcal{O}_F : \mathbb{Z}| = |\mathcal{O}_F : \mathbb{Z}[\alpha]| \cdot |\mathbb{Z}[\alpha] : \mathbb{Z}| = 3,$$

then D must be odd.

If $D > 1$, then $3 \mid D$. Since $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha + 2] = \mathbb{Z}[a]$, we choose to work with the latter at this stage. Since $3 \mid D$, there must exist a $\beta \in \mathbb{Z}[a]$ such that

$$\beta = \frac{b_0 + b_1 a + b_2 a^2}{3},$$

where 3 does not divide all of the b_j for $j = 0, 1, 2$. Suppose that $3 \mid b_0$, but $3 \nmid b_1$. Then $\beta - 1 = (b_1a + b_2a^2)/3 \in \mathcal{O}_F$. Also, $\gamma = b_1a^2/3 = (\beta - 1)a - a^3b_2/3 \in \mathcal{O}_F$ since $a/3$ is an algebraic integer given that it is a root of

$$(x - 2)^3 + 2 = x^3 - 6x^2 + 12x - 6.$$

Therefore,

$$3^3 N_F(\gamma) = N_F(3\gamma) = N_F(b_1a^2) = b_1^3 N_F(a)^2 = 4b_1^3,$$

so $3 \mid b_1$, a contradiction. The other cases such as $3 \mid b_1$ but $3 \nmid b_0$ are handled similarly. Thus, $D = 1$, $\text{disc}\{1, \alpha, \alpha^2\} = \Delta_F$, and $\mathbb{Z}[\alpha] = \mathcal{O}_F$.

Brett Tangedal has observed that the solution to Exercise 4.57 provided on page 448 is incorrect. The error occurs on line 10 where it is stated that $\mathcal{V}_1 = 1$. Indeed $\mathcal{V}_1 = \text{Gal}(F/\mathbb{Q})$. It can be shown (by an argument using Exercise 4.61, left to the reader) that $\text{Gal}(F/\mathbb{Q})$ has only one subgroup of order p^{r-1} where $|\text{Gal}(F/\mathbb{Q})| = p^r$. Thus, by Exercise 4.58(b), we have the result.