TYPOS TO BE CORRECTED IN THE THIRD PRINTING OF ANT

PAGE NUMBER	LINE NUMBER	MISPRINT→CORRECTION
5	2	unity,→unity, for odd n:
9	11	Exercise 1.1.→Exercise 1.1, which is a criterion for a $\mathbb{Z}$-module to be an ideal.
12	Exercise 1.13	$\mathbb{Z}[i]. \to \mathbb{Z}[i]$ with $a, b \in \mathbb{N}$.
14	8	$g(x) \in F[x] \to g(x) \in \mathbb{C}[x]$
19	2	$\in \mathfrak{O}_F$→is an algebraic integer in F
19	Theorem 1.29	See below[1]
26;27	-1;2,4,6,8	$\sum_{j=1}^{d} \to \sum_{i=1}^{d}$ **and** $\sum_{i=1}^{n/d} \to \sum_{j=1}^{n/d}$ for every occurrence on each line
27	-9	$\in F[x] \to \in \mathbb{Q}[x]$
27	-8	where $F \subseteq \mathbb{C}$ is a field and → where
29	9	$a^2(\frac{\sqrt{\Delta}}{a})^2 = b^2 - 4ac \to -a^2(\frac{\sqrt{\Delta}}{a})^2 = -(b^2 - 4ac)$
29	10	$\mathrm{disc}(f) \to -\mathrm{disc}(f)$
32	2	an integral polynomial→a monic integral polynomial
33	1	1.22→1.21
33	8–11	Replace the m_j by x_j for $j = 1, 2, \ldots, d$
35	-7	$(\alpha_i - \alpha_j) \to (\alpha_j - \alpha_i)$
36	5	square→square of a nonzero rational number
36	11	$q_{i.k} \in F \to q_{i,k} \in \mathbb{Q}$ **and** $\det(q_{i,k}) \to \det(q_{i,k}) \in \mathbb{Q}$, $D \neq 0$,
36	11	$q_{i,k} \to q_{k,i}$ (3 times)
37	14	$d \to D$
37	14	$\begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix}$
37	16, 18	interchange $q_{1,2}$ and $q_{2,1}$
39	5	$D^2\mathrm{disc}(\mathcal{B}_2) \to D^2\mathrm{disc}(\mathcal{B}_1)$
39	9	$\mathfrak{O}_F \to \mathfrak{O}_F$ as a $\mathbb{Z}$-module
40	6	$r\beta_1 \to \delta$
42	4	$\mathbb{Z}[\alpha] = \mathfrak{O}_F \to \alpha \in \mathfrak{O}_F$
44	2	$\alpha_i^2, \ldots, \alpha_i^n \to \alpha_i^{(2)}, \ldots, \alpha_i^{(n)}$ (*not* to be confused with the *powers* of α_i)
45	3–5	see below[2]
46	2	$z \in \mathbb{Z}$ →nonzero $z \in \mathbb{Z}$
46	3	$\alpha_i, \alpha_j \in R \to \alpha_1, \ldots, \alpha_d \in R$
46	4	$(\alpha_i - \alpha_j) \to (\alpha_j - \alpha_i)$
49	-8	$N_F(\alpha_j) \to \lvert N_F(\alpha_j) \rvert$
50	3	α is one → α is an associate of one
50	13	$\alpha_r = \beta_s \to \alpha_r = \beta_s w$ (where w is a unit)
54	4	page 31,→page 31, and Exercise 1.84 on page 52,
55	19	since $1/\lambda = 1 - \zeta_3^2 \to$ by Exercise 1.14, Equation (1.96), and the fact that $\zeta_3 \equiv 1 \pmod{\lambda}$
56	2,6,7,8,9	$u_3 \to u_4$
64	-1	$\sqrt{R - 4Q}. \to \sqrt{R - 4Q}$ for an appropriate choice of α and β.

---

[1] Add the following to the end of the proof of Theorem 1.29 for the sake of clarification: To see how the one-to-one property follows from this, suppose that $\theta_j(f(\alpha)) = \theta_j(g(\alpha))$. Then $f(\alpha_j) = g(\alpha_j)$, so as in the above $f(x) - g(x) = h(x)m_{\alpha_j,\mathbb{Q}}(x)$. Thus, $f(\alpha) - g(\alpha) = h(\alpha)m_{\alpha_j,\mathbb{Q}}(\alpha) = 0$ since $\theta(\alpha) = \alpha_j$.

[2] Replace the sentence "Since. . .= $(-1)^{r_2} \det(\alpha_i^j)$." with the following: Then $\det\left(\overline{\alpha_i^j}\right) = a - b\sqrt{-1}$, where the overline bar denotes complex conjugation. Since complex conjugation will leave the real rows of the determinant unchanged, and will interchange the $2r_2$ "non-real" rows in pairs corresponding to the conjugate embeddings, the value of $\det\left(\overline{\alpha_i^j}\right)$ is also $(-1)^{r_2}(a + b\sqrt{-1})$.

PAGE NUMBER	LINE NUMBER	MISPRINT→CORRECTION
72	10	$x - y \equiv \rightarrow y - x \equiv$
73	14	Exercise 1.9→Exercises 1.9 and 1.17
75	12	$\geq 1/2 \rightarrow > 1/2$
75	-3	$x = 1 \rightarrow x = \epsilon$
76	2	$\geq 1 + (r_1 - 1/\epsilon)^2 \rightarrow \geq 1 + (r_1 - 1)^2$
76	4	delete $\geq 2 + (r_1 - 1/\epsilon)^2$
76	5	penultimate→last
76	-9,-10	that there exists… $t \in \mathbb{Z} \rightarrow$ that for any $t \in \mathbb{Z}$ there exists a $x + y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ such that
78	21	$D \equiv 1 \pmod 4 \rightarrow D \equiv 1 \pmod 8$
83	5–6	Replace "and 1.69 on page 46, $\Delta_F = \pm N_F(\Phi'_n(\zeta_n))$" by: and Theorem 1.63, $\Delta_F \mid N_F(\Phi'_n(\zeta_n))$
83	-6	Δ_F is a power→ $\lvert\Delta_F\rvert$ is a power
84	15	$j \rightarrow \ell$ (6 times)
84	-7	stronger→stronger in the case where $n = p^a$
88	-3 (above footnotes)	Definition A.66→Remark A.67
89	-9	$\mathcal{U}_F \rightarrow \mathcal{R}_F$ (3 times)
91	16	$n = 4q \rightarrow \zeta_n = \zeta_{4q}$ **and** $n = p^2 \rightarrow \zeta_n = \zeta_{p^2}$
92	10	of $\mathcal{R}_F \rightarrow \mathcal{R}_F$
93	-5 (above footnotes)	$r_j \leq 1 \rightarrow r_j < 1$
93	-2 (above footnotes)	$= \det(\ell_j) \rightarrow = \lvert\det(\ell_j)\rvert$
93	2 (of Footnote 2.12)	Russion→Russian
94	-10 (above footnotes)	$\leq r_1 \rightarrow \leq r$
94	-4,-1 (above footnotes)	$\ell \rightarrow r_1\ell$
95	2	subset→subgroup
95	16	$r_j\beta_j \quad (r_j \in \mathbb{R}) \rightarrow t_j\beta_j \quad (t_j \in \mathbb{R})$
95	18	$\lfloor r_j \rfloor \beta_j \rightarrow \lfloor t_j \rfloor \beta_j$
96	-2 (above footnotes)	so→where $\mathcal{P}_{-z} = \{x - z : x \in \mathcal{P}\}$, so
98	1	Corollary 2.51→Lemma 2.51
98	19	there exists→with $\det(r_{i,j}) \neq 0$, there exists
98	-3	$\det(r_{i,j}) \rightarrow \lvert\det(r_{i.j})\rvert$ (twice)
99	5	$x_j \rightarrow x_i$
99	6	of Corollary 2.52→of (the complex version of) Corollary 2.52
99	-8 (above footnote)	$= \mathbb{R}^2 \rightarrow = \mathbb{Z}^2$
102	-1,1	delete: ", since $n = r_1 + 2r_2 + 1$ in this case"
102	8	$\frac{2^{r_1}\pi^{r_2}}{(r_1+2r_2)!} \rightarrow \frac{2^{r_1}}{(r_1+2r_2)!}$
102	9	delete: "and $n = r_1 + 2r_2$,"
102	10,12,14	$n \rightarrow r_1 + 2r_2$
102	-9	define→define B such that
102	-5	$+\epsilon \rightarrow +\epsilon 2^{r_1}(\pi/2)^{r_2}/n!$
102	-4	inequality→equality
102	-2	$\theta(\alpha) \rightarrow \Theta_F(\alpha)$
103	17	$\Delta_F \geq \rightarrow \lvert\Delta_F\rvert \geq$
104	5	$(\frac{e^2\pi}{4})^n \rightarrow (\frac{e^2\pi}{4})^n(2\pi n)^{-1}$
104	-5,-6,-7 (above footnote)	$d \in \mathbb{N} \rightarrow d \in \mathbb{Z}$
104	-2	$\Delta_F > d \rightarrow \lvert\Delta_F\rvert > \lvert d\rvert$
104	-3	$> d \rightarrow > \lvert d\rvert$
105	1	$\leq d \rightarrow \leq \lvert d\rvert$
105	2	$d = 1 \rightarrow \lvert d\rvert = 1$
105	5	$\Delta_F = d \rightarrow \Delta_F = -d$

PAGE NUMBER	LINE NUMBER	MISPRINT→CORRECTION
107	10	$\mathcal{P} \in \mathcal{S} \cap \mathbb{Z} \to \mathcal{P} \in \mathcal{S} \cap \mathbb{Z}^n$
109	12	$\sum_{j=1}^{r_1} +2 \to \sum_{j=1}^{r_1} x_j + 2$
110	21	$j = r_1 + 1, \ldots, r_2 \to j = r_1 + 1, \ldots, r_1 + r_2$
111	15, -3	$r_2 \to r_1 + r_2$
112	1	such that →such that for all k
112	2	$\theta_j \to \theta_k$
112	8	$\lvert\theta_j(\alpha)\ell_j\rvert \to \lvert\theta_j(\alpha)\ell_j\rvert^2$
112	-9	$a_j \to a_1$
113	2	$\ell_1(\theta_j(u_1)) \to \ell_1(\theta_1(u_1))$
113	-11	independent vectors→independent
114	1	$i = 1, \to j = 1,$
118	4 of footnote	$\exp \to \exp^{1/2}$
124	-3	$\equiv 2^{108} \to \equiv 2^{(103)5}$
129	12	nonzero ideal→ideal
129	-6 (above footnote)	$J = \mathcal{O}_F \to J = R$
130, 138	-10, -8 (above footnotes)	Condition C→Condition A
137	-7	every maximal→every nonzero maximal
143	2	some α →some irreducible α
146	-2	prime,→prime, $a \in \mathbb{Z}$,
146	-2	such that $p < \sqrt{\lvert\Delta_F\rvert}/2$ is a rational prime→ where the prime $p < \sqrt{\lvert\Delta_F\rvert}/2$ when $\Delta_F > 0$ and $p < \sqrt{\lvert\Delta_F\rvert/2}$ when $\Delta_F < 0$
154	-7	$\alpha = \to I =, \in \mathcal{P} \to \subseteq \mathcal{P}$, **and** $\alpha^{-1} \in \to I^{-1} \subseteq$
154	-6	$1 = \alpha\alpha^{-1} \in \mathcal{P}\mathcal{P}^{-1} \to R = II^{-1} \subseteq \mathcal{P}\mathcal{P}^{-1}$
165	Footnote	See below[3]
184	13	A function→A one-to-one function
200	11	$\sum_{j=1}^{g} \to \sum_{k=1}^{g}$
201	5	$\lvert\mathbb{Q}(\sqrt[3]{2})\rvert \to \lvert\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\rvert$
337	Figure 5.157	$P + Q = R \to P + Q = -R$
337	-8,-9	Delete: "We find the intersection. . .new point R."
339	6	$(x_3, y_3) \to (x_3, -y_3)$
339	16	$(x_3, -y_3) \to (x_3, y_3)$
339	-6	**Rational→Torsion**
345	-10 (above footnote)	$\lfloor n \rfloor \to \lfloor \sqrt{n} \rfloor$
348	3–4	factoring small· · ·digits).→finding small prime factors (those with no more than forty digits) of large composite numbers.
349	3 (after table)	$662278\ \mathbb{Z}/n\mathbb{Z} \to 662278 \in \mathbb{Z}/n\mathbb{Z}$
354	20	$= \{1\} \to = \varnothing$
354	-5 (above footnote)	set H → nonempty set H
355	6	Corollary A.20→Theorem A.20
358	7	and F^* is →, then any finite subgroup of $F^\times$,
358	8	,then F^* is cyclic→is cyclic
358	-2 (above footnote)	$n \in \mathbb{N} \to n \in N$
366	-4,-5 (above footnote)	cannot be. . . or $\deg_R(f) = \deg_R(h)$.→cannot be the product of two nonconstant polynomials.
373	7	$n \in \mathbb{N}$ roots in $\mathbb{C}$, where $d \geq n \geq 1 \to$ factors into a product of d linear factors in $\mathbb{C}[x]$
382	4	fourteen→sixteen
392	21	$5^2 - 1 \to 5^s - 1$
406	9	Remove the exponent 2 (twice)
406	14	$(\alpha/\beta - \gamma) \to f(\alpha/\beta - \gamma)$
419	-5 (above footnote)	$\alpha^d + c_{d-1}\alpha^{d-1} \to x^d + c_{d-1}x^{d-1}$

---

[3] On page 165, Footnote 3.13 should be deleted and replaced by the following: This is the largest known discriminant for which the class number of a complex quadratic field has exponent 2. See [51, Chapter 4, pp. 105–147] for the connection with prime-producing quadratic polynomials. Another instance of a complex quadratic field with exponent 2 is given in Example 3.80.

PAGE NUMBER	LINE NUMBER	MISPRINT→CORRECTION
424	-12	Lagrange's Theorem. . . 355) →Theorem A.20 on page 355
429	8	Insert before "By Exercise 3.18,..." the following:
		Choose $\alpha_j \in \mathcal{P}_j^{a_j} - \mathcal{P}_j^{a_j+1}$ for $j = 1, 2, \ldots, r$.
429	17	Condition C of Definition 3.9→Exercise 3.12
430	15	Exercise 3.8→Exercise 3.6

As a result of comments from David J. Smith of Auckland N.Z., I have decided to rewrite the proof of Theorem 1.77 on pages 42–43, as follows to clarify the situation:

Let $\alpha \in \mathfrak{O}_F$. The reader may verify that we may assume without loss of generality:

$$\alpha = \frac{a + b\sqrt{D}}{c}, \text{ where } \gcd(a, b, c) = 1, \tag{1.78}$$

with $a, b, c \in \mathbb{Z}$, $c > 0$, and

$$m_{\alpha,\mathbb{Q}}(x) = \left(x - \left(\frac{a + b\sqrt{D}}{c}\right)\right)\left(x - \left(\frac{a - b\sqrt{D}}{c}\right)\right) \in \mathbb{Z}[x].$$

Therefore,

$$T_F(\alpha) = \frac{2a}{c} \in \mathbb{Z}, \tag{1.79}$$

and

$$N_F(\alpha) = \frac{a^2 - b^2D}{c^2} \in \mathbb{Z}. \tag{1.80}$$

By Exercise 1.77 on page 47, $c \bigm| 2$.

If $c = 2$, then $2 \nmid ab$ by (1.78)–(1.80), so $1 \equiv a^2 \equiv b^2D \pmod 4$, and this holds if and only if $D \equiv 1 \pmod 4$. Hence, if $D \not\equiv 1 \pmod 4$, then $c = 1$. Therefore,

$$\mathfrak{O}_F = \mathbb{Z}[\sqrt{D}]$$

and if $D \equiv 1 \pmod 4$, then

$$\mathfrak{O}_F = \mathbb{Z}[(1 + \sqrt{D})/2]$$

since

$$\frac{a + b\sqrt{D}}{2} = \frac{a - b}{2} + b\left(\frac{1 + \sqrt{D}}{2}\right) \in \mathfrak{O}_F$$

for odd a, b.

Hence, by Definitions 1.60 and 1.74, if $D \not\equiv 1 \pmod 4$, then

$$\Delta_F = \operatorname{disc}(\{1, \sqrt{D}\}) = \det\begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}^2 = (-2\sqrt{D})^2 = 4D,$$

and if $D \equiv 1 \pmod 4$, then

$$\Delta_F = \operatorname{disc}(\{1, (1 + \sqrt{D})/2\}) = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{D}}{2} & \frac{1-\sqrt{D}}{2} \end{pmatrix}^2 = (-\sqrt{D})^2 = D,$$

as required. □

Also, this requires changing the solution of Exercise 1.77 on page 414 to read as follows.

If $c \nmid 2$, then by (1.79) there is a prime $p \bigm| a$ and $p \bigm| c$. By (1.80), $p^2 \bigm| b^2D$. However, $\gcd(a, b, c) = 1$, so $p^2 \bigm| D$. This is a contradiction since D is squarefree. Thus, $c \bigm| 2$.

Thanks go to Jerry M. Metzger, Bruce Dearden and Robby Wieler who pointed out numerous of the above clarifications since the appearance of the second printing of ANT. This is greatly appreciated and will help to polish the product for the third printing. They also asked numerous questions about the proof of Theorem 1.107 on pages 59–61, which caused me to revise the proof for greater clarity as follows.

On page 60, replace everything from "Thus, by part (b) of" on line 5 up to and including ... "and that $-2^{m-1} \equiv m \pmod 7$" on line 7 by the following.

"We claim that $U_m = -1$. If $U_m = 1$, then $\alpha^m - \beta^m = \alpha - \beta$. Thus, since $\alpha\beta = 2$ and $\alpha^2 = (1-\beta)^2$, then $\alpha^2 \equiv (1-\beta)^2 \equiv 1 \pmod{\beta^2}$. Therefore, $\alpha^m \equiv \alpha(\alpha^2)^{(m-1)/2} \equiv \alpha \pmod{\beta^2}$. However, $\alpha^m = \alpha - \beta + \beta^m$, so $\alpha - \beta \equiv \alpha \pmod{\beta^2}$, which implies that $\beta \equiv 0 \pmod{\beta^2}$, a contradiction. Hence, we have shown that $U_m = -1$. Thus, by Exercise 1.100(b), $-2^{m-1} = \sum_{j=1}^{(m+1)/2} \binom{m}{2j-1} 7^{j-1}$, so $-2^{m-1} \equiv m \pmod 7$. Moreover, $-2^{m-1} \equiv m \pmod 7$"

Delete everything from "By part (b) of Exercise 1.100," on line 13 up to and including the displayed equation on line 17. Then immediately after the displayed equation on line -8, delete "Therefore," and replace it by: "Thus, by successively raising α to the powers 7, $7^2, \ldots, 7^\ell$, then to the power $(m_1 - m)/7^\ell$, we see that:"

The proof of Theorem 2.26 on pages 81–82 actually requires some ideal theory that I do not introduce until Chapter Three. Thus, replace the proof with the following:

We may let $\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ by Theorem 1.18.

Claim 2.27 $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) = 0$ for any prime $p \nmid n$.

If $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) \neq 0$, then $g(\zeta_n^p) = 0$, so ζ_n is a root of $g(x^p)$. By Theorem 1.18 again, $g(x^p) = m_{\zeta_n,\mathbb{Q}}(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let $f(x) = \sum_j a_j x^j \in \mathbb{Z}[x]$ have image $\overline{f}(x) = \sum_j \overline{a_j} x^j$ under the natural map

$$\mathbb{Z}[x] \mapsto (\mathbb{Z}/p\mathbb{Z})[x].$$

Thus, $\overline{g}(x^p) = \overline{m}_{\zeta_n,\mathbb{Q}}(x)\overline{h}(x)$. However, $\overline{g}(x^p) = \overline{g}^p(x)$ since $\operatorname{char}(\mathbb{Z}/p\mathbb{Z}) = p$. Therefore,

$$0 = \overline{g}(\zeta_n^p) = (\overline{g}(\zeta_n))^p = \overline{g}(\zeta_n).$$

Since $\Phi_n(x) \bigm| (x^n - 1)$, then

$$x^n - 1 = \Phi_n(x)k(x) = m_{\zeta_n,\mathbb{Q}}(x)g(x)k(x),$$

for some $k(x) \in \mathbb{Z}[x]$. Therefore, in $\mathbb{Z}/p\mathbb{Z}[x]$,

$$x^n - \overline{1} = \overline{x^n - 1} = \overline{m}_{\zeta_n,\mathbb{Q}}(x)\overline{g}(x)\overline{k}(x).$$

Since $\overline{g}$ and $\overline{m}_{\zeta_n,\mathbb{Q}}$ have a common root ζ_n, then $x^n - \overline{1}$ has a repeated root. However, this is impossible by Exercise C.8(b) on page 401 since $p \nmid n$. We have shown that ζ_n^p is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ for any prime $p \nmid n$. Repeated application of the above argument shows that y^p is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ whenever y is a root. Hence, ζ_n^j is a root of $m_{\zeta_n,\mathbb{Q}}(x)$ for all j relatively prime to n such that $1 \leq j < n$. Thus, $\deg m_{\zeta_n,\mathbb{Q}} \geq \phi(n)$. However, $m_{\zeta_n,\mathbb{Q}}(x) \bigm| \Phi_n(x)$, so $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$.

Replace: "Since ... $L = J$" in lines -6 to -2 of page 133 of the proof of Corollary 3.17 with the following:

Hence, for all $\beta \in J$, there exists a $\gamma \in L$ such that $\beta\alpha = \gamma\alpha$. Therefore, $(\beta - \gamma)\alpha = 0$ where $\alpha \neq 0$ since I is nonzero. Thus, since we are in an integral domain $\beta - \gamma = 0$, namely $\beta = \gamma$. We have shown that $J \subseteq L$. A similar argument shows that $L \subseteq J$.

Replace the proof of Theorem 3.37 on page 146 with the following:

Since $\prod_{j=1}^r \mathcal{P}_j^{a_j} = \cap_{j=1}^r \mathcal{P}_j^{a_j}$ by Exercise 3.15, then the isomorphism (3.38) follows from the Chinese Remainder Theorem given in Exercise 3.18.

G. Eilenberger pointed out that although Theorem A.16 on page 354 is not incorrect, it can mislead the non-expert, so it should be sharpened. In fact, I decided to simplify it considerably so there could be no confusion. Replace the statement of the theorem with the following:

If G is a finite abelian group, then any two decompositions of G into a direct product of cyclic groups of prime power order contain the same number of multiplicands of each order.

The solution of part (b) of Exercise 3.23, given on page 429 needs to be fixed. Replace the proof by the following:

If $r \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$, then there exist $m_1, m_2 \in \mathbb{N}$ such that $r^{m_1} \in I$ and $r^{m_2} \in J$. Therefore, $r^{m_1+m_2} = r^{m_1} r^{m_2} \in IJ$. This shows that $\mathrm{rad}(I) \cap \mathrm{rad}(J) \subseteq \mathrm{rad}(IJ)$. Also, since $IJ \subseteq I \cap J$, then $\mathrm{rad}(IJ) \subseteq \mathrm{rad}(I \cap J)$. We have shown that

$$\mathrm{rad}(I) \cap \mathrm{rad}(J) \subseteq \mathrm{rad}(IJ) \subseteq \mathrm{rad}(I \cap J).$$

Hence, the required equalities will follow if we show that $\mathrm{rad}(I \cap J) \subseteq \mathrm{rad}(I) \cap \mathrm{rad}(J)$. If $r \in \mathrm{rad}(I \cap J)$, then there exists an $n \in \mathbb{N}$ such that $r^n \in I$ and $r^n \in J$, so $r \in \mathrm{rad}(I)$ and $r \in \mathrm{rad}(J)$, which means that $r \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$, as required.

Thanks go to my students: Kyle Bothwell, Andrew Culham, Craig Hawkins, Andy Kirsch, Collette Lemieux, Polina Sabinin, and Thea van Roode, in the grad. course offered from ANT in the winter 2001 term, who contributed to the above corrections as did Philippe Pitteloud of M.I.T.