Fields and Galois Theory: Errata

John M. Howie

December 2006

Page 6:
In Theorem 1.4, R should be a commutative ring *with unity*.

Page 39:
In Theorem 2.15 (i), the polynomials f and g must be *non-zero*.

Page 44:
In Line 15, $p(X)$ must be non-constant. In Theorem 2.24 (Gauss's Lemma) the polynomial f must also be non-constant.

Page 44:
In the proof of Gauss's Lemma, remark that g' and h' can be chosen so that $\partial g' = \partial g$ and $\partial h' = \partial h$.

Page 46:
In the statement of Theorem 2.27 (Eisenstein's Criterion) the first sentence should be:
Let
$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$
be a polynomial, where $a_0, a_1, \ldots, a_n$ are integers with greatest common divisor equal to 1.

Page 65:
The final sentence of Theorem 3.23 should be:
Then there is an isomorphism ψ, an extension of φ, from $K[\alpha]$ onto $K'[\alpha']$, and $\psi(\alpha) = \alpha'$.

Page 80:
Line 2 should read:
(ii) f does not split completely over any subfield E such that $K \subset E \subset L$.

Page 102:
In the line after (7.22), the reference should be to (7.20) rather than (7.21).

Page 107:
The first few lines of he proof of Theorem 7.18 should read:
(i) Let $\{z_1, z_2, \ldots, z_n$ be a basis for L over K. Each z_i is algebraic over K, with minimum polynomial m_i (say). Let $m = m_1m_2 \ldots m_n$ and let N be a splitting

filed for m over L. Then N is also a splitting field for m over K, since L is generated over K by some of the roots of m in N. By the proof of ...

Page 107:
Before the statement of Corollary 7.19 we need a definition. Let L be a field containing subfields K_1, K_2. The subfield $K_1(K_2) = K_2(K_1)$ is the smallest subfiled of L containing $K_1 \cup K_2$, and is denoted by $K_1 \vee K_2$, the **join** of K_1 and K_2. More generally, the smallest subfield of L containing the union of subfields $K_1, K_2, \ldots, K_n$ is called the **join** of $K_1, K_2, \ldots, K_n$ and is denoted by

$$K_1 \vee K_2 \vee \cdots \vee K_n \,.$$

Page 108:
The proof of Corollary 7.19 should be as follows: By the theorem just proved, we may suppose that $L = K(z_1, z_2, \ldots, z_n)$, that $m_1, m_2, \ldots, m_n$ are (respectively) the minimum polynomials of $z_1, z_2, \ldots, z_n$, and that N is a splitting field over K for the polynomial $m_1 m_2 \ldots m_n$. Let $i \in \{1, 2, \ldots, n\}$ and let z_i be an arbtrarily chosen root of m_i. Since z_i and z_i' are both roots of m_i, there is a K-isomorphism from $K(z_i)$ onto $K(z_i')$. By Corollary 7.14, this isomorphism extends to a K-automorphism φ of N. Note that $z_i' \in \varphi(L) \simeq L$. Hence every root of m_i is contained in a subfield L' of N such that L' contains K and is K-isomorphic to L. Since N is generated over K by the roots of m, it is generated by (finitely many) subfields containing K and isomorphic to L. □

Page 111:
Line 5 should read: ... if $p \not| r$. (Omit "only if".)

Page 122:
Line –7 should read: In Chapters 8 and 10 we shall need ...

Page 122:
The statement of Theorem 7.36 should mention that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f.

Page 123:
Line –10 should read : G, since each γ in H fixes the elements of M, ...

Page 132:
In Line 5, delete "irreducible".

Page 132:
In Line –10, replace Theorem 7.19 by Lemma 7.19.

Page 134:
Line 5 should read $X^{p-1} + X^{p-2} + \cdots + X + 1$

Page 135:
Restate Theorem 8.9 thus: Let K be a field of characteristic 0 containing mth roots of unity, where $m \geq 2$. Let $K_0(\simeq \mathbb{Q})$ be the prime subfield of K. Then, for every divisor d of m (including m itself), the cyclotomic polynomial Φ_d lies in $K_0[X]$.

Page 136:
In Remark 8.10, the reference should be to Exercise 8.5.

Page 138 :
Theorem 8.13 should read: Let K be a field of characteristic zero, and let L be a splitting field over K of the polynomial $X^m - 1$. Then $\mathrm{Gal}(L : K)$ is isomorphic to a subgroup of R_m, the multiplicative group of residue classes $\bar{r} \pmod m$ such that $(r, m) = 1$.
Its proof is:

We may suppose without loss of generality that $\mathbb{Q} \subseteq K$. Suppose first that $K = \mathbb{Q}$. Let ω be a primitive mth root of unity in L, and let $\sigma \in \mathrm{Gal}(L, \mathbb{Q})$. We know that $\sigma(\omega)$ must also be a primitive mth root of unity and so

$$\sigma \in \mathrm{Gal}(L, \mathbb{Q}) \text{ if and only if } \sigma(\omega) = \omega^{r_\sigma}\,, \text{ where } (r_\sigma, m) = 1\,. \tag{8.12}$$

Since $\omega^r = \omega^s$ if and only if $r \equiv s \pmod m$, we have a one-one map from $\mathrm{Gal}(L, \mathbb{Q})$ onto R_m, the multiplicative group of residue classes $\bar{r} \bmod m$ such that $(r, m) = 1$.

Let $\sigma, \tau \in \mathrm{Gal}(L, \mathbb{Q})$. Then

$$(\sigma\tau)\omega = \sigma(\omega^{r_\tau})^{r_\sigma} = \omega^{r_\sigma r_\tau} = \omega^{r_\tau r_\sigma} = (\tau\sigma)(\omega), \tag{8.13}$$

and so $Gal(L, \mathbb{Q})$ is abelian. The other consequence of (8.13) is that the map $\sigma \mapsto \bar{r}_\sigma$ is a homomorphism, since $\sigma\tau$ maps to $\bar{r}_\sigma \bar{r}_\tau$. It is clear that the map is one-one,.

Now let us replace $\mathbb{Q}$ by a more general field K of characteristic zero. From Theorem 7.36, the Galois group of L over K is the Galois group of $\mathbb{Q}(\omega)$ over $K \cap \mathbb{Q}(\omega)$, and so is isomorphic to a subgroup of the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, that is, to a subgroup of R_m. $\square$

Page 139:
Lines 2 and 3 should read: . . . is isomorphic to a subroup of the multiplicative group. . .

Page 140:
In Line −4, “monomorphisms” should be “homomorphisms”.

Page 147:
To match the solution, Exercise 8.9 should be concerned with $X^6 + 3$ rather than $X^6 - 3$.

Page 170:
Line 8 should read

$$K \subseteq E = M_r \subseteq M_{r-1} \subseteq \cdots \subseteq M_0 = M.$$

Also, in Line 15, the word “irreducible” should be omitted.

Page 172:
In Lines 7, 8, 12, 14, 18 and 19, M should be replaced by M_1.

http://www.springer.com/978-1-85233-986-9

Fields and Galois Theory
Howie, J.M.
2006, X, 226 p. 22 illus., Softcover
ISBN: 978-1-85233-986-9