Chapter 15.1

Lemma 1.5 in this chapter states:

Lemma (Gauss). Let $f(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x)$ is reducible over $\mathbb{Q}$ if and only if $f(x)$ is reducible over $\mathbb{Z}$.

Also Lemma 1.6 in this chapter states:

Lemma. If $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, then it is also reducible over $\mathbb{Z}$.

Although the statements are are correct, we propose the following alternative and slightly more general statement from the notes:

Lemma 3.6 (Gauss Lemma). Let $f(X) \in \mathbb{Z}[x]$ with $\deg(f) \geq 1$. Then the following are equivalent.

(1) $f(x)$ is irreducible over $\mathbb{Z}$.

(2) $f(x)$ is primitive and irreducible over $\mathbb{Q}$.

For a proof see the notes.

Chapter 16.3

Problem 3 in this chapter states:

Problem 3. Show that $f(x) \in F[x]$ has a root α of multiplicity $n > 1$ if and only if $f^{(k)}(\alpha) = 0$, $k = 1, \ldots, n-1$, and $f^{(n)}(\alpha) \neq 0$ where $f^{(i)}(\alpha)$ is the ith derivative of $f(x)$ at $x = \alpha$ as defined in Problem 2.

The way this is stated, both directions as false. We demonstrate with two counterexamples.

First we recall Example 9.4 from the notes. Let $f(x) = x^3 - 2 \in \mathbb{Z}_3[x]$. Then

$$(x-2)^3 = x^3 - 6x^2 - 12x - 8 = x^3 - 2 = f(x),$$

and so $f(x)$ has 2 as a root with multiplicity $n = 3 > 1$. However we have

$$f'(x) = 3x^2, \quad f''(x) = 6x, \quad f'''(x) = 6 = 0$$

and so $f'(2) = f''(2) = f'''(2) = 0$. This shows that the straight direction of Problem 3 fails since $f^{(3)}(2) = 0$.

For the other direction, consider the polynomial $g(x) = x^2 + 1 \in \mathbb{Q}[x]$. Then $g'(x) = 2x$ and $g''(x) = 2$. We have that

$$g'(0) = 0, \quad g''(0) = 2$$

and so the second statement of Problem 3 holds for $n = 2$. However, $g(x)$ does not have 0 as a root with multiplicity 2 (it does not have 0 as a root at all). This shows that the converse direction of Problem 3 fails.

To make the converse direction work, one only needs to assume additionally that $f(\alpha) = 0$, that is that α is a root of $f(x)$. To make the straight direction work one needs to be more careful with the characteristic of a field. For a more general statement in this context we propose the following statement from the notes:

Theorem 9.3. Let $f(x) \in F[x]$ with $\deg(f) \geq 1$. Let E be a splitting field of $f(x)$ over F. Let $\alpha \in E$ be a root of $f(x)$ with multiplicity m_f. Let $m \geq 1$. Then the following are equivalent.

(1) $f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ and $f^{(m)}(\alpha) \neq 0$.

(2) $m = m_f$ and either $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p > m$.

For a proof see the notes.

Chapter 18.5

Theorem 5.9 in this chapter states:

Theorem 5.9 If $u \in K_m$, where $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_m$ is an ascending tower of fields K_i such that $[K_i : K_{i-1}] = 2$, then u is constructible.

Equivalently, if $[\mathbb{Q}(u) : \mathbb{Q}] = 2^t$ for some $t > 0$, then u is constructible.

The last statement in this theorem is wrong. We propose the following slightly more general statement from the notes:

Theorem 17.9. The following are equivalent.

(1) $z \in \mathbb{K}$ is constructible.

(2) There exists a sequence of field extensions $\mathbb{Q} = k_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ such that $z \in K_n$ and for every $1 \leq i \leq n$ we have $[K_i : K_{i-1}] = 2$. In particular it follows that $K_i = K_{i-1}(z_i)$ for some z_i with $z_i^2 \in K_{i-1}$.

If moreover any of (1) or (2) holds, then the following also holds.

(3) There exists $t \in \mathbb{Z}$, $t \geq 0$ such that $[\mathbb{Q}(z) : \mathbb{Q}] = 2^t$.

For a proof see the notes. Theorem 5.9 in the book claims that (3) implies (1), which is false, that is, there exist $u \in \mathbb{C}$ such that $[\mathbb{Q}(u) : \mathbb{Q}]$ is a power of 2, but u is not constructible. For a counterexample, see Problem 15 in Problem Set 6.

Furthermore, this claim is used later in the book when proving that a regular n-gon is constructible if and only if $\phi(n)$ is a power of 2. In that proof it is claimed that to show that $u = \cos \frac{2\pi}{n}$ is constructible, it suffices to show that $[\mathbb{Q}(u) : \mathbb{Q}] = 2^k$, $k \geq 0$, which is false. For the correct proof of this statement see the proof of Corollary 17.14 in the notes.