Undergraduate Algebra
Notes and Exercises

John Peloquin

Chapter IV

§ 3

Exercise (6)**.** Let K be a subfield of a field E. Let $f, g \in K[t]$ with f irreducible in $K[t]$. Suppose there exists $\alpha \in E$ such that $f(\alpha) = 0 = g(\alpha)$. Then $f|g$ in $K[t]$.

Proof. Let $\mathrm{ev}_\alpha : K[t] \to E$ be the homomorphism induced by evaluation at α and let $J = \ker \mathrm{ev}_\alpha$. By assumption, we have $f, g \in J$. Since $K[t]$ is a principal ring (Theorem 2.1), $J = (h)$ for some $h \in K[t]$. Now in $K[t]$, $h|f$ and $h|g$, but since f is irreducible we must also have $f|h$, so $f|g$. $\square$

§ 5

Exercise (4 (Rational root theorem))**.** Let $f(t) = a_n t^n + \cdots + a_0 \in \mathbb{Z}[t]$ with $a_n \neq 0$ and $n \geq 1$. If $f(b/c) = 0$ with $b, c \in \mathbb{Z}$, $c \neq 0$, and $(b, c) = 1$, then $b|a_0$ and $c|a_n$.

Proof. We may assume without loss of generality that f is primitive. Since $f(b/c) = 0$, we know $(t - b/c)|f$ in $\mathbb{Q}[t]$. But by Gauss (Theorem 5.3), this implies $(ct - b)|f$ in $\mathbb{Z}[t]$ since $(b, c) = 1$. Therefore $c|a_n$ and $b|a_0$. $\square$

Remark. In particular if $a_n = 1$, then all rational roots of f are integral.

Exercise (9)**.** Let R be a factorial ring and K the quotient field of R. Let

$$f(t) = t^d + c_{d-1} t^{d-1} + \cdots + c_0 \in R[t] \qquad (d \geq 2)$$

Let $p \in R$ be prime and let

$$g(t) = f(t) + p/p^{nd} \in K[t] \qquad (n \geq 1)$$

Then g is irreducible in $K[t]$.

Proof. Define $h(t) = p^{nd} g(t/p^n)$. By direct computation,

$$h(t) = t^d + p^n c_{d-1} t^{d-1} + \cdots + p^{n(d-1)} c_1 t + p^{nd} c_0 + p \in R[t]$$

By Gauss (Theorem 6.7), it is sufficient to prove that h is irreducible in $R[t]$. But this follows from Eisenstein (Theorem 6.10) since p divides all except the leading coefficient and p^2 does not divide the constant coefficient. $\square$

Remark. Let $R = \mathbb{Z}$ so $K = \mathbb{Q}$. Observe that $g(t) \to f(t)$ as $n \to \infty$. Therefore there are irreducible polynomials arbitrarily close to f, with roots arbitrarily close to those of f. In particular, if f has exactly $d-k$ distinct real roots, then g also has exactly $d-k$ distinct real roots for n sufficiently large. (See Exercise 7.)

Chapter VII

§ 1

Exercise (11)**.** Let F be a field, E a finite extension of F, and F' an arbitrary extension of F, with E and F' both contained in some common extension. Then the composite EF' is finite over F', and

$$[EF' : F'] \leq [E : F]$$

Proof. Since E/F is finite, it is finitely generated and algebraic (Theorem 1.1). Suppose $E = F(\alpha)$ with α algebraic over F. We claim $EF' = F'(\alpha)$. Indeed, by definitions both are the smallest extensions of F containing F' and α, so they are equal. Now α is trivially algebraic over F' since it is algebraic over F, so $F'(\alpha)/F'$ is finite and

$$[EF' : F'] = [F'(\alpha) : F'] = \deg_{F'} \alpha \leq \deg_F \alpha = [F(\alpha) : F] = [E : F]$$

since simple algebraic extensions are finite (Theorem 1.3) and the minimal polynomial of α over F' must divide the minimal polynomial of α over F. The general case $E = F(\alpha_1, \cdots, \alpha_k)$ now follows by induction and application of the tower law (Theorem 1.4). $\square$

Exercise (12)**.** Let F be a field and let E_1 and E_2 be finite extensions of F with relatively prime degrees over F, both contained in some common extension. Then the composite $E_1 E_2$ is finite over F and

$$[E_1 E_2 : F] = [E_1 : F][E_2 : F]$$

Proof. Since E_1E_2/E_2 is a translation of the finite extension E_1/F, it follows that E_1E_2/E_2 is finite and $[E_1E_2 : E_2] \le [E_1 : F]$ (Exercise 11). Now by the tower law (Theorem 1.4), E_1E_2/F is finite and

$$[E_1E_2 : F] = [E_1E_2 : E_2][E_2 : F]$$

By symmetry,

$$[E_1E_2 : F] = [E_1E_2 : E_1][E_1 : F]$$

Since $[E_1 : F]$ and $[E_2 : F]$ are relatively prime, $[E_1 : F]$ divides $[E_1E_2 : E_2]$, so $[E_1E_2 : E_2] = [E_1 : F]$ as desired. □

Remark. This result shows that translation of a finite extension over a finite extension of relatively prime degree preserves degree. Because degree is an isomorphism type for finite extensions (viewed as finite dimensional vector spaces), this result is analogous to a diamond isomorphism theorem.

§ 3

Exercise (6)**.** Let F be a field of characteristic 0 and A an algebraic extension of F such that for all $f \in F[t]$ with $\deg f \ge 1$ there exists $\alpha \in A$ with $f(\alpha) = 0$. Then A is algebraically closed.

Proof. Let $f(t) = a_n t^n + \cdots + a_0 \in A[t]$ with $a_n \ne 0$ and $n \ge 1$. Let α be a root of f in some extension of A (Theorem 2.2). We claim $\alpha \in A$. Observe α is algebraic over F since $\alpha \in F(a_1, \ldots, a_n, \alpha)$, an algebraic extension of F (Theorem 1.4). Let K be a splitting field for the minimal polynomial of α over F in some extension of A (Theorem 3.1) so that $\alpha \in K$. Since F has characteristic 0, $K = F(\gamma)$ for some primitive element $\gamma \in K$ (Theorem 2.5). Now by assumption the minimal polynomial of γ over F has a root $\gamma' \in A$, and $K = F(\gamma') \subseteq A$ since K is normal (Theorems 3.3–4). Therefore $\alpha \in A$ as desired. □

§ 4

Remark. In the proof of Theorem 4.5 on p. 285, to prove that the restriction map $G_{KE/E} \to G_{K/(K\cap E)}$ is surjective observe that the image is a subgroup whose fixed field is $K \cap E$. Indeed, clearly $K \cap E$ is fixed, and if $\alpha \in K - K \cap E$, then $\alpha \in KE - E$, so there exists $\sigma \in G_{KE/E}$ with $\sigma\alpha \ne \alpha$. But then $\sigma|_K \alpha \ne \alpha$. By the Galois correspondence (Theorem 4.2), this subgroup must be $G_{K/(K\cap E)}$.

Chapter VIII

§ 1

Remark. $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m|n$. Indeed, if $m|n$ and $\alpha \in \mathbb{F}_{q^m}$, we claim $\alpha^{q^{mk}} = \alpha$ for all k. For $k = 1$ this holds since $\mathbb{F}_{q^m}$ consists of the roots of $t^{q^m} - t$ (Theorem 1.2). For $k > 1$ we have by induction

$$\alpha^{q^{mk}} = \alpha^{q^{m(k-1)+m}} = \alpha^{q^{m(k-1)}q^m} = \left(\alpha^{q^{m(k-1)}}\right)^{q^m} = \alpha^{q^m} = \alpha$$

Now in particular $\alpha^{q^n} = \alpha$, so $\alpha \in \mathbb{F}_{q^n}$ (Theorem 1.2) as desired. Conversely, if $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, then by the above and the tower law we have

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}][\mathbb{F}_{q^m} : \mathbb{F}_q]$$

But $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ and $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$ (Theorem 1.1), so $m|n$ as desired.

Exercise (1)**.** Let $g(t) = t^{q^n} - t$.

(a) If $f \in \mathbb{F}_q[t]$ is irreducible of degree m, then $f|g$ if and only if $m|n$.

(b) If I_m is the set of monic irreducible polynomials of degree m over $\mathbb{F}_q$,

$$g(t) = \prod_{m|n} \prod_{f \in I_m} f(t)$$

(c) If $\psi(m)$ is the size of I_m,

$$q^n = \sum_{m|n} m\psi(m)$$

(d) If μ is the Möbius function, then

$$\psi(n) = \frac{1}{n} \sum_{m|d} \mu(m) q^{n/m}$$

Proof.

(a) Let α be a root of f, so $m = \deg_{\mathbb{F}_q} \alpha$. Then $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ by uniqueness of finite fields. Now $f|g$ if and only if α is a root of g, which holds if and only if $\alpha \in \mathbb{F}_{q^n}$ (Theorem 1.2), which holds if and only if $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, which holds if and only if $m|n$ by the above remark.

(b) Immediate from (a).

(c) Immediate from (b) and degrees of the polynomials.

(d) Immediate from (c) and Möbius inversion. □

§ 2

Remark. We already know the structure of finite cyclic groups. Specifically, if $G = \langle x \rangle$ is the cyclic group of order n, then the subgroups are just $\langle x^m \rangle$ for $m|n$, and $\langle x^m \rangle \subseteq \langle x^k \rangle$ if and only if $k|m$ (Theorem II.5.4). Galois theory for finite fields gives us an order reversing correspondence between the subfields of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ and the subgroups of the automorphism group $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, which is cyclic of order n, generated by the Frobenius automorphism (Theorems 2.3–4). Therefore it follows that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m|n$. This is just a field theoretic translation of a group theoretic fact, by way of the Galois correspondence.

References

[1] Lang, Serge. *Undergraduate Algebra, 3rd ed.* Springer, 2005.