Notes and exercises from *Abstract Algebra*

John Peloquin

Introduction

This document contains notes and exercises from [1].

Chapter I

Section 4

In addition to Propositions 4.9 and 4.10, the following is useful (see for example the proof of Theorem II.9.12):

Proposition. *Let G be a group, $N \trianglelefteq G$ and $N \subseteq H, K \leq G$. Then H and K are conjugate in G if and only if H/N and K/N are conjugate in G/N.*

Chapter II

Section 5

The argument used in the proof of Proposition 5.10 is essentially Frattini's:

Proposition (Frattini)**.** *Let G be a finite group, $H \trianglelefteq G$, and P a Sylow p-subgroup of H. Then $G = HN_G(P)$.*

Proof. If $g \in G$, then $gPg^{-1} \subseteq gHg^{-1} = H$ since $P \subseteq H \trianglelefteq G$. But gPg^{-1} is also a Sylow p-subgroup of H, and all Sylow p-subgroups of H are conjugate in H (Theorem 5.7), so there is $h \in H$ with

$$hgP(hg)^{-1} = h(gPg^{-1})h^{-1} = P$$

Therefore $hg \in N_G(P)$, $g \in HN_G(P)$, and $G = HN_G(P)$. $\square$

The key observation is that since all conjugates of P in G are contained in H, they are also conjugate in H. Proposition 5.10 follows as a corollary:

Corollary. *Let G be a finite group, P a Sylow p-subgroup of G, and $N_G(P) \subseteq H \leq G$. Then $N_G(H) = H$.*

Proof. Note $N_G(H)$ is finite, $H \trianglelefteq N_G(H)$, and P is a Sylow p-subgroup of H, so $N_G(H) = HN_{N_G(H)}(P) \subseteq HN_G(P) \subseteq HH = H$ by Frattini. □

Section 9

Remark. In the proof of Lemma 9.11, $G = N \rtimes A = N \rtimes B$ (Proposition 11.2). In particular, each $b \in B$ can be expressed uniquely in $N \rtimes A$ in the form $b = ua$ with $u \in N$ and $a \in A$. Then $u = u_a$ in Grillet's notation, and $u_{aa'} = u_a(au_{a'}a^{-1})$ follows from the multiplication rule in $N \rtimes A$. In this way, N acts as a "bridge" between A and B.

Section 10

Commutator subgroups satisfy the following universal mapping property:

Proposition. *Let G be a group, $H \trianglelefteq G$, and $K = [G, H]$ the subgroup of G generated by commutator elements $[x, y] = xyx^{-1}y^{-1}$ with $x \in G$ and $y \in H$. Then $K \trianglelefteq G$. If $\pi : G \to G/K$ is the canonical projection, then $\pi(H) \subseteq Z(\pi(G))$, and if $\varphi : G \to L$ is a homomorphism with $\varphi(H) \subseteq Z(\varphi(G))$, then φ factors uniquely through π; that is, there exists $\psi : G/K \to L$ unique such that $\varphi = \psi \circ \pi$:*

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/K \arrow[d, dashed, "\psi"] \\ & L \end{tikzcd}$$

Proof. By the universal mapping property for quotient groups (Theorem I.5.1), since $K \subseteq \ker \varphi$. □

This is a generalization of the universal mapping property noted in Section 9, where $H = G$ (see Proposition 9.1 and Exercise 9.7). It is implicit in the proofs of Propositions 10.1 and 10.3.

Chapter IV

Section 5

Remark. In Proposition 5.1(2), if K is finite then $m = 0$ and q is separable.

Section 6

We sketch an alternative approach to purely inseparable extensions starting with polynomials having only one distinct root:

Definition. A nonconstant polynomial $f(X) \in K[X]$ is *purely inseparable* if

$$f(X) = a(X-\alpha)^m \in \overline{K}[X]$$

where $a \in K$, $\alpha \in \overline{K}$, and $m > 0$.

Note f is both separable and purely inseparable if and only if f is linear.

Proposition. *Let $f(X) = a(X-\alpha)^m \in K[X]$ be purely inseparable as above.*

1. *If K has characteristic 0, then $\alpha \in K$.*
2. *If K has characteristic $p \neq 0$, then $\alpha^{p^k} \in K$ for some $k \geq 0$ with*

$$f(X) = a\big(X^{p^k} - \alpha^{p^k}\big)^{m/p^k}$$

Proof. By the binomial theorem,

$$f(X) = a(X-\alpha)^m = aX^m - am\alpha X^{m-1} + \cdots \in K[X]$$

so $am\alpha \in K$ and $m\alpha \in K$ since $a \neq 0$. If K has characteristic 0, then $m \neq 0$ in K and $\alpha \in K$. If K has characteristic $p \neq 0$, then either $\alpha \in K$ or else $p|m$ and

$$f(X) = a\big((X-\alpha)^p\big)^{m/p} = a\big(X^p - \alpha^p\big)^{m/p}$$

Repeating this argument with α^p in place of α, we must eventually find $k \geq 0$ with $\alpha^{p^k} \in K$ and $f(X)$ as claimed. □

Proposition. *Let $q(X) \in K[X]$ be monic irreducible and purely inseparable. If K has characteristic 0, then $q(X) = X - a$ for some $a \in K$. If K has characteristic $p \neq 0$, then $q(X) = X^{p^k} - a$ for some $a \in K$ and $k \geq 0$.*

Proof. By Proposition 5.1 and the above. In the case of characteristic $p \neq 0$, $q(X) = s(X^{p^k})$ for s separable and purely inseparable, hence linear. $\square$

Definition. An element α is *purely inseparable over* K when α is algebraic over K and $\mathrm{Irr}(\alpha : K)$ is purely inseparable.

Definition. An algebraic extension E of K is *purely inseparable over* K when every element of E is purely inseparable over K.

These definitions are compatible with those in the text. In particular:

Corollary. *An extension E of K is both separable and purely inseparable over K if and only if $E = K$. In particular if K has characteristic* 0 *or K is finite, then K is the only purely inseparable extension of K.*

Corollary. *If K has characteristic $p \neq 0$ and E is a purely inseparable extension of K in $\overline{K}$, then*

$$E \subseteq K^{1/p^\infty} = \left\{ \alpha \in \overline{K} \mid \alpha^{p^k} \in K \textit{ for some } k \geq 0 \right\}$$

Section 7

Remark. In the proof of Proposition 7.2, we obtain the polynomial identity

$$\Phi(P) = A_m^n B_n^m \prod_{i,j} (R_i - S_j)$$

in $\mathbb{Z}[A_m, B_n, R_1, \ldots, R_m, S_1, \ldots, S_n]$. Substituting $A_m \mapsto a_m$, $B_n \mapsto b_n$, $R_i \mapsto \alpha_i$, and $S_j \mapsto \beta_j$ on both sides, we obtain

$$D = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$$

Indeed, let M be the matrix in $M_{m+n}(\mathbb{Z}[A_m, \ldots, A_0, B_n, \ldots, B_0])$ defining P, so $P = \det M$. Since Φ is a ring homomorphism, $\Phi(P) = \det \Phi(M)$, where $\Phi(M)$ is the result of applying Φ to the entries of M. Since the determinant is a natural transformation, the result of the substitution above on $\Phi(P)$ is the determinant of the result of the substitution on the entries of $\Phi(M)$, which is D:

$$\Phi(P)(a_m, b_n, \alpha_i, \beta_j) = \det\left[\Phi(M)(a_m, b_n, \alpha_i, \beta_j)\right] = D$$

Section 9

Temporarily, we say that an extension E of K is *separable$_0$* if it is separable in the sense defined in Section 5, and *separable$_1$* if it is separable in the sense defined in Section 9.

Proposition. *An algebraic extension is separable$_0$ if and only if it is separable$_1$.*

Proof. Let E be an algebraic extension of K.

If E is separable$_0$ over K and $K \subseteq F \subseteq E$ is any intermediate field, then the empty set is a separating transcendence base for F over K since F is separable$_0$ over K. Therefore E is separable$_1$ over K.

Conversely if E is separable$_1$ over K, recall that E is a directed union of finitely generated intermediate fields $K \subseteq F \subseteq E$ (Exercise 2.1). By assumption each such F has a separating transcendence base over K which is empty since F is algebraic over K, so F is separable$_0$ over K. Since the directed union of separable$_0$ extensions is separable$_0$ (Proposition 5.11), E is separable$_0$ over K. $\square$

The above proof works for all field characteristics. In the case of characteristic 0, the result also follows from the fact that every algebraic extension is separable$_0$ (Proposition 5.5), so every transcendence base is separating and hence *every* extension is separable$_1$! In characteristic $p \neq 0$, the result also follows from Proposition 9.6 and Theorem 9.7.

Remark. In the proof of Proposition 9.6, we can avoid appealing to the primitive element theorem (Proposition 5.12) by arguing that if $K(\alpha_1, \dots, \alpha_n)$ is separable$_0$ over K then it is linearly disjoint from K^{1/p^∞} by induction on n, making use of this diagram and Proposition 9.4:

$$\begin{tikzcd}[arrows=dash]
 & & K(\alpha_2, \dots, \alpha_n)^{1/p^\infty} \arrow[d] \\
K(\alpha_1, \dots, \alpha_n) \arrow[d] & & K(\alpha_2, \dots, \alpha_n)K^{1/p^\infty} \arrow[d] \\
K(\alpha_2, \dots, \alpha_n) \arrow[urr] \arrow[dr] & & K^{1/p^\infty} \arrow[dl] \\
 & K &
\end{tikzcd}$$

Chapter V

Section 7

Remark. The tower property for the norm (Proposition 7.5) is equivalent to the fact that the determinant of the determinant of an $n \times n$ matrix of commuting $m \times m$ matrices is equal to the determinant of the original matrix when viewed as an $mn \times mn$ block matrix—see [2].

Chapter VI

Section 1

Question. In an ordered field, when is it the case that every positive element is a sum of squares?

- In $\mathbb{Q}$ it is true, for example by Lagrange's four-square theorem: if $p = m/n$ where m, n are positive integers, then we can write

  $$mn = a^2 + b^2 + c^2 + d^2$$

  where a, b, c, d are nonnegative integers, and therefore

  $$p = \left(\frac{a}{n}\right)^2 + \left(\frac{b}{n}\right)^2 + \left(\frac{c}{n}\right)^2 + \left(\frac{d}{n}\right)^2$$

- In $\mathbb{R}$ it is also true, since if $x > 0$ then $x = (\sqrt{x})^2$.

- In $\mathbb{Q}(\sqrt{2})$ under the ordering from $\mathbb{R}$, $\sqrt{2}$ is positive but it is not a sum of squares because there is another ordering of $\mathbb{Q}(\sqrt{2})$ under which $\sqrt{2}$ is negative.

References

[1] Grillet, P. A. *Abstract Algebra*, 2nd ed. Springer, 2007.

[2] Ingraham, M. H. "A note on determinants." 1937.