Summer Term Abstract Algebra
Samir Siksek
Handouts I–IV; 55 pages in total
`https://samirsiksek.github.io/siksek.github.io/index.html`
Errata and comments by Darij Grinberg

The page numbers below refer to the printed page numbers in each handout; thus the pagination restarts at page 1 four times. The four supplied PDFs are dated April 30, April 28, May 18, and May 28, 2020, respectively. This list is not claimed to be exhaustive. It concentrates on mathematical errors, proof gaps, and points likely to cause avoidable difficulty for a student. The corrections to references into *Introduction to Abstract Algebra* use the version dated September 22, 2020.

Most of the errata below were found with assistance from GPT-5.6 Sol. All have been verified by myself.

A. Handout I: Finite Fields

1. **Page 1, opening of Section 2:** In the September 22, 2020 version of *Introduction to Abstract Algebra*, rings and fields are Chapters XIV and XV, not Chapters XV and XVI.

2. **Page 2, opening list of facts:** The assertion "$\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime" needs the usual hypothesis $m \geq 2$ (or, at least, that m is a positive integer).

3. **Page 3, Theorem 2:** The quotient q and remainder r are *unique*, as in the real-polynomial division theorem recalled just above. Thus replace "Then there are $q, r \in K[X]$ with" by "Then there are unique $q, r \in K[X]$ with".

4. **Page 5, opening of Section 4:** In the September 22, 2020 version of *Introduction to Abstract Algebra*, quotients of additive abelian groups are treated in Chapter XII, not Chapter XIII.

5. **Page 6, Exercise 5:** For the same version of *Introduction to Abstract Algebra*, the cited result is Lemma XII.17, not Lemma XIII.17.

6. **Page 9, proof of Theorem 12(c):** After writing $f = f_1 f_2$, the literal equality "$\gcd(f, f_1) = f_1$" requires f_1 to have been chosen monic, since polynomial gcds are being normalized to be monic. It is enough to say that $\gcd(f, f_1)$ has positive degree, and hence is not 1.

   At the end of the proof, "composite" should be "reducible".

7. **Page 10:** Again, "composite" (in "The first three are composite") should be "reducible".

8. **Page 12, reduction of θ^{n+1}:** In the long displayed computation, replace "$-a_1\theta - a_1\theta^2 - \cdots - -a_{n-2}\theta^{n-1}$" by "$-a_0\theta - a_1\theta^2 - \cdots - a_{n-2}\theta^{n-1}$".

B. Handout II: Cosets and Lagrange's Theorem

1. **Page 8, Example 15:** In the September 22, 2020 MA136 notes, the parity result is Theorem XIII.40, not Theorem XIV.40.

2. **Page 11, opening of Section 10:** Replace "We checked that $\mathrm{GL}_2(K)$ is a group and $\mathrm{SL}_n(K)$ is a subgroup" by "We checked that $\mathrm{GL}_n(K)$ is a group and $\mathrm{SL}_n(K)$ is a subgroup".

C. Handout III: Cyclic and Dihedral Groups

1. **Pages 8–9, derivation of the rotation matrix:** The polar angle ϕ is not determined when the vector $\mathbf{x}$ is zero. After introducing the polar coordinates (r, ϕ), add that ϕ may be chosen arbitrarily when $r = 0$ (or handle the zero vector separately).

2. **Page 11, opening of Section 6:** In the September 22, 2020 version of *Introduction to Abstract Algebra*, the notation for the symmetries of the square is in Section IV.4, not Section V.4.

3. **Page 13, display (4):** Delete the extra closing brace after "$r^{n-1}s$".

D. Handout IV: Symmetric Groups

1. **Page 1, opening of Section 2:** In the September 22, 2020 version of *Introduction to Abstract Algebra*, symmetric groups are Chapter XIII, not Chapter XIV.

2. **Page 7, definition of orbit:** It is worth pointing out that $\mathrm{Orb}_\rho(a)$ can also be written as
$$\mathrm{Orb}_\rho(a) = \left\{a, \rho(a), \rho^2(a), \ldots\right\},$$
because the equality $\rho^u(a) = a$ entails that the sequence $\left(a, \rho(a), \rho^2(a), \ldots\right)$ is periodic with period u. This equality is used in the proof of Lemma 12 further below (e.g., when you derive $b \in \mathrm{Orb}_\rho(a)$ from $b = \rho^k(a)$, and likewise when you derive $\rho^{k+t}(a) \in \mathrm{Orb}_\rho(a)$).

3. **Page 8, proof of Theorem 8:** Replace "$\{1, 2, \ldots, n\} = C_1 \cup C_2 \cup \cdots \cup C_n$" by "$\{1, 2, \ldots, n\} = C_1 \cup C_2 \cup \cdots \cup C_k$".

4. **Pages 12–13, Theorem 19 and Corollary 20:** These are only true if $n \geq 2$. For $n = 1$, one has $A_1 = S_1$, so $[S_1 : A_1] = 1$ and $\#A_1 = 1$, not $1!/2$.

5. **Page 15, first permutation-type example:** Replace "has permutation type $[4, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]$" by "has permutation type $[4, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0]$" (the tuple must have 11 entries, not 12, so it had one 0 too much at the end).

6. **Page 15, equation (9):** Insert the missing plus sign after $3\alpha_3$. The equation should read
$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n = n.$$