ALGEBRA 2: EXERCISES

You are encouraged to discuss the HW with other students, but you are to write up your own solutions. At the top of your HW solution paper, you are to print your name **legibly**, and to write and sign the following anti-plagiarism oath:

I did not copy these solutions from another source.

§1. Rings and subrings: Exercises.

1.1. Let R be a ring with an additive identity denoted by 0, and a multiplicative identity denoted by 1. Prove the following.
   (a) If $z \in R$ so that $z + a = a$ for all $a \in R$, then $z = 0$.
   (b) If $a, b, c \in R$ so that $a + b = 0$ and $a + c = 0$, then $b = c$.
   (c) If $u \in R$ so that $u \cdot a = a$ for all $a \in R$, then $u = 1$.
   (d) For any $a \in R$, we have $0 \cdot a = 0$.
   (e) With -1 the additive inverse of 1, we have $-1 \cdot a = -a$ for any $a \in R$.
   (f) $0 = 1$ if and only if $R = \{0\}$.

1.2. Let R be a ring, and suppose $u \in R$ is a unit. Suppose $v, w \in R$ so that $uv = uw = 1$. Show that $v = w$.

1.3. Let $p \in \mathbb{Z}$ be prime, and let

$$S = \left\{ \frac{a}{b} : \ a, b \in \mathbb{Z}, \ p \nmid b \right\}.$$

Show that S is a subring of $\mathbb{Q}$.

1.4. Let R, R' be rings. For $(a, a'), (b, b') \in R \times R'$, we define

$$(a, a') + (b, b') = (a + b, a' + b'), \ (a, a') \cdot (b, b') = (ab, a'b').$$

Show that, with these operations, $R \times R'$ is a ring.

1.5. Fix $d \in \mathbb{Z}$ so that d is not a square. Set $R = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z} \}$.
   (a) Show that R is a subring of $\mathbb{C}$.
   (b) Define $N : R \to \mathbb{Z}$ by $N(a + b\sqrt{d}) = a^2 - db^2$. Show that for all $x, y \in R$, we have $N(xy) = N(x)N(y)$.

1.6. Let ω be a complex number so that $\omega^3 = 1$, $\omega \neq 1$.
   (a) Show that ω is a root of the polynomial

$$(X - 1)(X^2 + X + 1)$$

   and deduce that ω is a root of $X^2 + X + 1$.
   (b) Let $R = \{a + b\omega : \ a, b \in \mathbb{Z} \}$. Show that R is a subring of $\mathbb{C}$.
   (c) Show that for $x, y \in \mathbb{Z}$, we have

$$x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y).$$

1.7.

(a) Suppose R is a ring with subrings S, T. Show that $S \cap T$ is a subring of R.

(b) Suppose R is a ring with subrings $S_1, S_2, S_3, \ldots$. Show that

$$\cap_{i=1}^{\infty} S_i$$

is a subring of R.

§2. Homomorphisms, ideals, and quotient rings: Exercises.

2.1. Say $\varphi : R \to R'$, $\psi : R' \to R''$ are homomorphisms. Show that $\psi \circ \varphi : R \to R''$ is a homomorphism.

2.2. Let $\varphi : R \to R'$ be a homomorphism. Show that $\varphi(R)$ is a subring of R'.

2.3. Let $\varphi : R \to R'$ be a homomorphism. Then $\ker\varphi$ is an additive subgroup of R, with the property that for $a \in R,\ x \in \ker\varphi$, we have $ax \in \ker\varphi$.

2.4.

(a) Let R be a ring, and take $a \in R$. Then with

$$(a) = aR = \{ax :\ x \in R\ \},$$

show (a) is an ideal of R.

(b) Let R be a ring, and take $a, b \in R$. Then with

$$(a, b) = \{ax + by :\ x, y \in R\ \},$$

show (a, b) is an ideal of R.

(c) Let $I = \{f \in \mathbb{Q}[X] :\ f(\sqrt{5}) = 0\ \}$. Show that I is an ideal of $\mathbb{Q}[X]$.

2.5. Let I be an ideal of a ring R.

(a) Show that multiplication in R/I is well-defined.

(b) For $x \in R$, show that $-(x + I) = -x + I$.

2.6. Let I be an ideal of a ring R, and define $\varphi : R \to R/I$ by $\varphi(a) = a + I$. Show that φ is a surjective homomorphism with kernel I.

2.7. Suppose I, J are ideals of a ring R. Show that $I + J$ is also an ideal of R.

§3. Basic homomorphism theorems: Exercises.

3.1. Let R, R' be rings, $\varphi : R \to R'$ a homomorphism. Let $K = \ker\varphi$, and define $\psi : R/K \to R'$ by $\psi(a + K) = \varphi(a)$.
   (a) Show that ψ is well-defined; that is, show that if $a+K = b+K$ then $\psi(a+K) = \psi(b + K)$.
   (b) Show that ψ is a homomorphism.

3.2. Say $\varphi : R \to R'$ is a surjective homomorphism.
   (a) Suppose I is an ideal of R, and set $I' = \varphi(I)$. Show that for any $a' \in I'$ and $x' \in R'$, we have $-a' \in I'$ and $x'a' \in I'$.
   (b) Suppose I' is an ideal of R'. Set $I = \varphi^{-1}(I')$. Show that for any $a \in I$ and $x \in R$, we have $-a \in I$ and $xa \in I$.
   (c) Suppose I' is an ideal of R' and $I = \varphi^{-1}(I')$. Show that $\ker\varphi \subseteq I$.
   (d) Let I' be an ideal of R'. Show that $I' \subseteq \varphi(\varphi^{-1}(I'))$.
   (e) Let I be an ideal of R containing $\ker\varphi$. Show that $\varphi^{-1}(\varphi(I)) \subseteq I$.

3.3. Suppose R is a ring.
   (a) Show that if I, J are ideals of R, then so is $I \cap J$.
   (b) Suppose $\{I_k\}_{k\in\mathbb{Z}_+}$ is a collection of ideals of R. Show that

$$\cap_{k=1}^{\infty} I_k$$

   is an ideal of R.

3.4. Let R be a ring with ideals $I \subseteq J$. Show that

$$(R/I)/(J/I) \simeq R/J.$$

   (Suggestion: To ease notation, let $\overline{a} = a + I$, $\overline{R} = R/I$, $\overline{J} = J/I$. Then define a map from $\overline{R}$ to R/J, and show that the map is a well-defined surjective homomorphism with kernel $\overline{J}$. Alternatively, you can define a map from R to $\overline{R}/\overline{J}$, and show this map is a surjective homomorphism with kernel J.)

3.5. Let R be a ring with subring S and ideal I.
   (a) Show that $S + I$ is a subring of R.
   (b) Show that I is an ideal of $S + I$.
   (c) Show that $S \cap I$ is an ideal of S.
   (d) Show that $(S + I)/I \simeq S/(S \cap I)$.

3.6. Suppose $\varphi : R \to S$, $\psi : R \to T$ are homomorphisms so that φ is surjective. Show that there is a homomorphism $\chi : S \to T$ so that $\psi = \chi \circ \varphi$ if and only if $\ker\varphi \subseteq \ker\psi$.

3.7. Suppose $p, q \in \mathbb{Z}$ are distinct primes. Define $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ by

$$\varphi(a) = (a + p\mathbb{Z}, a + q\mathbb{Z}).$$

(a) Show φ is a homomorphism.
(b) Find $\ker\varphi$.
(c) Knowing the cardinality of $\mathbb{Z}/\ker\varphi$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, show φ is surjective.

3.8. Suppose $\varphi : R \to R'$ is a homomorphism, and suppose $a \in R$, $a' \in R'$ so that $\varphi(a) = a'$. Show that

$$\{x \in R : \ \varphi(x) = a' \ \} = a + \ker\varphi.$$

3.9. Take $m, n \in \mathbb{Z}$. Define $\psi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $\psi(a) = (a + m\mathbb{Z}, a + n\mathbb{Z})$.
(a) Show ψ is a homomorphism.
(b) Find $\ker\psi$, and determine when ψ is surjective.

3.10. Suppose $\varphi : R \to R'$ is a homomorphism (so R, R' are rings), and $u \in R$ is a unit with multiplicative inverse v.
(a) Show that $\varphi(u)$ is a unit in R' with multiplicative inverse $\varphi(v)$.
(b) Show that if φ is an isomorphism and R is a field, then R' is a field.

§4. Integral domains and fields: Exercises.

4.1. Show that the units of a ring form a group under multiplication. (So with U the set of units of a ring R, you must show U is non-empty; U is closed under multiplication; every element of U has a multiplicative inverse in U.)

4.2. Suppose $R \neq \{0\}$ is a ring and u is a unit in R. Show that u is not a zero divisor.

4.3. Suppose R is an integral domain, and $a, b, c \in R$ so that $a \neq 0$ and $ab = ac$. Show that $b = c$.

4.4. Let R be a ring with ideal I.
   (a) Suppose I is a prime ideal; show that R/I is not the trivial ring (where the trivial ring is the ring with just one element).
   (b) Suppose I is a prime ideal. Show that R/I is an integral domain.
   (c) Suppose R/I is an integral domain. Show that I is a prime ideal.

4.5. Let R be a ring with ideal I.
   (a) Suppose I is a maximal ideal. Explain why R/I is not the trivial ring.
   (b) Suppose I is a maximal ideal. Show that R/I is a field.
   (c) Suppose R/I is a field. Show that I is maximal when R/I is a field.

4.6. Show that every maximal ideal is a prime ideal.

4.7. Let $\sim$ be the relation defined in Theorem 4.6.
   (a) Show that $\sim$ is an equivalence relation.
   (b) With Q defined as in Theorem 4.6, show that addition is well-defined on Q.

4.8. Suppose R is an integral domain with $a, b \in R$, $a, b \neq 0$. Show that $(a) = (b)$ if and only if $a = bu$ for some unit $u \in R$. Conclude that $(a) = R$ if and only if a is a unit in R.

4.9. Suppose R is not the trivial ring and $\varphi : R \to R'$ is an injective homomorphism
   (a) Suppose $x \in R$ is a zero divisor. Show that $\varphi(x)$ is a zero divisor in R'.
   (b) Suppose that φ is an isomorphism and R is an integral domain; show that R' is an integral domain.

§5. Euclidean domains, principal ideal domains, and unique factorisaton domains.

5.1. Let R be an integral domain.
(a) Show that for $a, b \in R$, $a, b \neq 0$, we have $(a) = (b)$ if and only if $a = bu$ where u is a unit.
(b) Show that for $a \in R$, we have $(a) = R$ if and only if a is a unit.

5.2. Let R be a Euclidean domain with the map δ. Suppose $a, b \in R$ so that neither is 0, and b is not a unit.
(a) Show that there are $q, r \in R$ so that $a = abq + r$ with $r \neq 0$ and $\delta(r) < \delta(ab)$.
(b) Show that $\delta(a) \leq \delta(r)$ (and hence $\delta(a) < \delta(ab)$).

5.3. Let R be a principal ideal domain, and take a, b to be nonzero elements of R. Take $c \in R$ so that $(a, b) = (c)$ (where $(a, b) = \{ax + by : \ x, y \in R\ \}$, which we have seen is an ideal). Explain why this means $c|a$ and $c|b$. Then suppose that $d \in R$ so that $d|a$ and $d|b$; show that $d|c$.

5.4. Let R be a principal ideal domain with ideals $I_1, I_2, I_3, \ldots$ so that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

Set $J = \cup_{k=1}^{\infty} I_k$.
(a) Show that J is an ideal of R.
(b) Show that there is some $n \in \mathbb{Z}_+$ so that $I_m = I_n$ for all $m \geq n$. (Suggestion: Focus on the fact that J is a principal ideal to show that $J \subseteq I_n$ for some n.)

5.5. Let R be a principal ideal domain, $p \in R$, $p \neq 0$.
(a) Suppose p is irreducible; show that (p) is a maximal ideal. (Suggestion: Suppose J is an ideal of R so that $(p) \subsetneq J \subseteq R$. Take $a \in J$ so that $a \notin (p)$; let

$$I = (p, a) = \{px + ay : \ x, y \in R\ \};$$

in another exercise, we saw I is an ideal of R. Now use the assumptions on R and p to show $I = R$; compare I to J to conclude $J = R$.)
(b) Suppose (p) is a prime ideal; deduce that p is irreducible. (Suggestion: Suppose $p = ab$ for some $a, b \in R$. Use the fact that (p) is a prime ideal to deduce that either a or b is a unit.)

5.6. Let R be a UFD, $a, b, c \in R$ nonzero. Take $d = \text{hcf}(a, b)$.

(a) Show that $a = dx$, $b = dy$ for some $x, y \in R$ so that $\text{hcf}(x, y) = 1$.

(b) Show that $\text{hcf}(ac, bc) = c \cdot \text{hcf}(a, b)$.

(c) Suppose that $\text{hcf}(a, b) = 1$ and $a|bc$; show that $a|c$.

5.7. Suppose R is a UFD.

(a) Suppose that $p \in R$ so that p is nonzero and not a unit. Show that p is irreducible if (p) is a prime ideal.

(b) Suppose that $p \in R$ so that p is nonzero and not a unit. Show that p is irreducible only if (p) is a prime ideal.

5.7. Suppose R, R' are integral domain and $\varphi : R \to R'$ is an isomorphism.

(a) Suppose R is a PID; show that R' is a PID. (Suggestion: Begin by taking an ideal I' of R' and set $I = \varphi^{-1}(I')$.)

(b) Suppose $x \in R$ so that $x \neq 0$ and x is reducible; show that $\varphi(x)$ is reducible.

§6. Gauss' Lemma and consequences: Exercises.

6.1. Suppose R is a unique factorisation domain (UFD), and

$$f = a_0 + a_1X + \cdots + a_mX^m,\ g = b_0 + b_1X + \cdots + b_nX^n$$

are nonzero elements of $R[X]$ so that

$$\text{hcf}(a_0, a_1, \ldots, a_m) = 1,\ \text{hcf}(b_0, b_1, \ldots, b_n) = 1.$$

Suppose p is an irreducible element of R that divides all the coefficients of fg; derive a contradiction. (Suggestion: Let s be the smallest index so that $p \nmid a_s$, and let t be the smallest index so that $p \nmid b_t$. Consider the $s+t$ coefficient of fg.)

6.2 Let R be a UFD, Q its field of fractions. Suppose f^* is primitive in $R[X]$, and $\alpha \in Q$ so that αf^* is also primitive in $R[X]$. Show that α is a unit in R. (Suggestion: Write $f^* = c_0 + c_1X + \cdots + c_nX^n$ where $c_i \in R$, and write $\alpha = \frac{a}{b}$ where $a, b \in R$. Argue that $b|\text{hcf}(c_0, \ldots, c_n)$; then argue that α must be an element of R, which is in fact a unit.)

6.3. Let R be a UFD, $f = a_0+a_1X+\cdots+a_nX^n \in R[X]$, f primitive. Suppose $p \in R$ is irreducible with $p|a_i$, $0 \le i < n$, $p^2 \nmid a_0$, $p \nmid a_n$. To show f is irreducible, we argue by contradiction: Assume $f = gh$ where $g, h \in R[X]$, $g = b_0 + b_1X + \cdots + b_rX^r$, $h = c_0 + c_1X + \cdots + c_sX^s$, $r, s \ge 1$.

(a) Show that $p|b_0$ or $p|c_0$, but not both. Also show that $p \nmid b_r$ and $p \nmid c_s$.

(b) Suppose $p|b_0$. Let k be the smallest positive integer so that $p \nmid b_k$. Show that $k < n$ and $p \nmid a_k$.

6.4. Let R be a UFD, a, b nonzero elements of R. Define $\text{lcm}(a, b)$ to be an element $t \in R$ so that $a|t$, $b|t$, and if $s \in R$ so that $a|s$ and $b|s$, then $t|s$. Show that $\text{lcm}(a, b)$ is well-defined up to units in R.

6.5. Prove that the following polynomials are irreducible over $\mathbb{Q}$; justify your answers.

$$f = 7X^4 - 18X^3 + 6X^2 - 24X + 12$$

$$g = 2X^3 - 5X + 25$$

6.6. (The purpose of this exercise is to show that a polynomial over $\mathbb{Q}$ can have a root modulo p for every prime p, but not have a root in $\mathbb{Q}$.) Take $f = (X^2+1)(X^2+2)(X^2-2) \in \mathbb{Q}[X]$, p an odd prime, and let $\overline{f}$ denote f modulo p. With $r = (p-1)/2$, we see that $\{\pm1, \pm2, \ldots, \pm r\}$ is a set of representatives of the nonzero integers modulo p, and so $1^2, 2^2, \ldots, r^2$ represent all the nonzero squares modulo p.

(a) Show that $0^2, 1^2, 2^2, \ldots, r^2$ are distinct modulo p.

(b) Let $\overline{a} = a + p\mathbb{Z}$. Show that

$$H = \{\overline{1}^2, \overline{2}^2, \ldots, \overline{r}^2\}$$

is a subgroup of $G = (\mathbb{Z}/p\mathbb{Z})^*$, where $(\mathbb{Z}/p\mathbb{Z})^*$ is the set of nonzero elements of $\mathbb{Z}/p\mathbb{Z}$. (Recall from Number Theory/Group Theory that $(\mathbb{Z}/p\mathbb{Z})^*$ is a group under multiplication.)

(c) Let G, H be as in (b). Suppose $\overline{a} \in G$, $\overline{a} \notin H$. Explain why $\overline{a}H \cap H = \emptyset$ and $G = \overline{a}H \cup H$.

(d) Suppose $\overline{a}, \overline{b} \in G$, $\overline{a}, \overline{b} \notin H$. Explain why $(\overline{b})^{-1}\overline{a}H = H$.

(e) Suppose still that $\overline{a}, \overline{b} \in G$, $\overline{a}, \overline{b} \notin H$. Explain why there is some $\overline{c} \in G$ so that $\overline{a}\overline{b} = \overline{c}^2$.

(f) Show that f has no root in $\mathbb{Q}$, but for each prime p, there is some $a \in \mathbb{Z}$ so that $f(a) \equiv 0 \pmod{p}$.

§7. Testing polynomials for irreducibility: Exercises.

7.1. Let R be an integral domain, and I a prime ideal of R. Define $\varphi : R[X] \to (R/I)[X]$ by

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$$

where $\overline{a}_j = a_j + I$.

(a) Show that φ is a surjective homomorphism.
(b) Suppose $g, h \in R[X]$. Show that deg $(gh) =$ deg $(g) +$ deg (h).
(c) Suppose $f \in R[X]$ is primitive with its leading coefficient not in I; show that if f is reducible in $R[X]$ then $\varphi(f)$ is reducible in $(R/I)[X]$.

7.2. Let R, R' be rings with $R \subseteq R'$; fix $\alpha \in R'$. Define $\varphi_\alpha : R[X] \to R'$ by

$$\varphi_\alpha(c_0 + c_1X + \cdots + c_nX^n) = c_0 + c_1\alpha + \cdots + c_n\alpha^n.$$

Show that φ_α is a homomorphism.

7.3. Suppose R is a UFD and $f \in R[X]$ such that deg $f > 0$ and f has a root $\alpha \in R$. Show that $f = (X - \alpha)g$ for some $g \in R[X]$. (Suggestion: Write $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots b_{n-1}X^{n-1}$ where $a_i \in R$, $b_i \in Q$ where Q is the field of fractions of R. Expand $(X - \alpha)g$ and use that $\alpha \in R$ and R is a ring to show that $b_{n-1}, \ldots, b_0 \in R$.)

7.4. Let $\mathbb{C}$ denote the field of complex numbers and $i = \sqrt{-1}$. For $\alpha = a + bi \in \mathbb{C}$, let $\overline{\alpha} = a - bi$, the complex conjugate of α. Define $\varphi : \mathbb{C} \to \mathbb{C}$ by $\varphi(\alpha) = \overline{\alpha}$.

(a) Show that φ is an isomorphism.
(b) Suppose $f \in \mathbb{R}[X]$ and $\alpha \in \mathbb{C}$ so that $f(\alpha) = 0$. Show that $f(\overline{\alpha}) = 0$.
(c) It is known that any $f \in \mathbb{C}[X]$ with deg $f > 0$ can be factored as a product of linear factors in $\mathbb{C}[X]$. Use this to show that if $f \in \mathbb{R}[X]$ is irreducible then deg $f = 1$ or 2.

7.5. Let p be a prime number in $\mathbb{Z}$, and

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Using the substitution $Y = X + 1$, show that f is irreducible in $\mathbb{Z}[X]$ (and hence in $\mathbb{Q}[X]$).

7.6. Let $f = X^3 + 3X^2 + 2X + 4 \in \mathbb{Z}[X]$; slightly abusing notation, we also write f for the image of f in $(\mathbb{Z}/p\mathbb{Z})[X]$ where p is a prime. Show that f is reducible in $(\mathbb{Z}/7\mathbb{Z})[X]$, but irreducible in $\mathbb{Z}[X]$.

7.7. Factor the following polynomials into products of irreducible factors in $\mathbb{Q}[X]$.

(a) $f = X^4 + 4X^3 + 5X^2 + 4X + 1$
(b) $g = X^3 + 4X^2 + 3X + 2$
(c) $h = X^4 + 3X^3 + 6X^2 + 3X - 12$

7.8. Write down all the irreducible polynomials of degree 2 or 3 in $(\mathbb{Z}/2\mathbb{Z})[X]$.

§8. Field extensions and algebraic elements: Exercises.

8.1. Suppose K, L are fields and $\varphi : K \to L$ is a homomorphism. Show that φ is injective.

8.2. Finish proving Proposition 8.2; so with the scalar product defined as in the proof of Proposition 8.2, you must show L is a vector space over K.

8.3. Suppose $M : L$ and $L : K$ are field extensions. Show that $M : K$ is a field extension.

8.4. Suppose that $L : K$ is a field extension and $\alpha \in L$ so that α is algebraic over K. Set

$$I = \{ f \in K[X] : \ f(\alpha) = 0 \ \}.$$

We have seen there is a monic polynomial that generates I; show that this polynomial is unique.

8.5. Let $L : K$ be a field extension, $\alpha \in L$ algebraic over K with $n = \deg \mathrm{m}_\alpha(K)$.

(a) Show that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a linearly independent set over K.

(b) Show that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans $K[\alpha]$ as a vector space over K. (Suggestion: Use induction on m to show that for $m \geq n$, α^m is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.)

(c) Show that $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$.

8.6. Let $L : K$ be a field extension, with $\alpha \in L$. Show that α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.

8.7. Let $L : K$ be a field extension, $\alpha \in L$ algebraic over K. Show that every element of $K(\alpha)$ is algebraic over K.

8.8. Suppose K, L are fields with $K \subseteq L$, and $\alpha \in L$ is algebraic over K. Suppose also that L' is another field and $\varphi : L \to L'$ is a homomorphism (and thus is necessarily injective). Set $K' = \varphi(K)$ and $\alpha' = \varphi(\alpha)$.

(a) Show that K' is a subfield of L'. (You may use results previously proved.)

(b) Extend $\varphi : L \to L'$ to the map $\widetilde{\varphi} : L[X] \to L'[X]$ by defining

$$\widetilde{\varphi}(a_0 + a_1 X + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n.$$

Show that $\widetilde{\varphi}$ is an injective homomorphism.

(c) Show that $\mathrm{m}_{\alpha'}(K') = \widetilde{\varphi}(\mathrm{m}_\alpha(K))$.

8.9. Say K, L_1, L_2, M are fields so that $K \subseteq L_1 \subseteq M$, $K \subseteq L_2 \subseteq M$, $[M : K] < \infty$, $[L_1 : K] = 3$, and $[L_2 : K] = 5$. Show that $[M : L_2]$ is divisible by 3.

§9. The characteristic of a field and finite fields: Exercises.

9.1. Let K be a field with $p = \mathrm{char}K$. Let $H = \{c{\cdot}1_K : \ c \in \mathbb{Z}\}$, and define $\varphi : \mathbb{Z} \to H$ by $\varphi(c) = c \cdot 1_K$. Recall that we have seen φ is a surjective homomorphism.
(a) Show that $\ker\varphi = (p)$.
(b) Use the Fundamental Homomorphism Theorem to show H is a field with p elements.

9.2. Let G be an abelian group with identity 1, and suppose $x \in G$ so that $\mathrm{ord}(x) = a < \infty$.
(a) Show that for $k \in \mathbb{Z}_+$, we have $x^k = 1$ if and only if $a|k$.
(b) Let $\langle x \rangle$ denote the cyclic subgroup of G generated by x; so

$$\langle x \rangle = \{x^m : \ m \in \mathbb{Z}\}.$$

Show that $|\langle x \rangle| = a$.

9.3. Let G be an abelian group, $x \in G$ with $\mathrm{ord}(x) = n < \infty$. Suppose $n = ab$ where $a, b \in \mathbb{Z}_+$ so that $\mathrm{hcf}(a, b) = 1$.
(a) Show that $\mathrm{ord}(x^a) = b$ and $\mathrm{ord}(x^b) = a$.
(b) Use the fact that $\mathrm{hcf}(a, b) = 1$ to show there exist $s, t \in \mathbb{Z}$ so that $x = yz$ where $y = x^{bt}$, $z = x^{as}$.
(c) With $x = yz$ where y, z are as in (b), show that $\mathrm{ord}(y) = a$ and $\mathrm{ord}(z) = b$.