Notes on Abstract Algebra & Algebraic Geometry

Akash Dhiraj

Euler Circle, Palo Alto, CA 94306
Email address: akashdhiraj2019@gmail.com
URL: https://akashdhiraj.com/

These notes are from algebra classes I took at Euler Circle. They contain problems on group theory, fields & Galois theory, and ring theory & algebraic geometry.

Textbook Used: [RS]

Contents

CHAPTER 0.1

Helpful Lemmas & Theorems

1. Groups

LEMMA 0.1.1. *If p is prime, a group of order p is cyclic, and it's generated by every non-identity element.*

PROOF. Let G be a group such that $|G| = p$. Then, consider a non-identity element $x \in G$. By Lagrange's theorem, $|x| = p$, and, hence, $\langle x \rangle = G$ because $\langle x \rangle \subset G$ and $|\langle x \rangle| = |G|$. Since our choice of x was arbitrary, we know all non-identity elements of G generate G. □

LEMMA 0.1.2. *All groups of order 4, must be isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

PROOF. Suppose we consider a group G (where $|G| = 4$) that contains an element g such that $|g| = 4$. Then, $G = \langle g \rangle$ must by cyclic and isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Now, consider a group H (once again, where $|H| = 4$) that doesn't contain an element of order 4. Then, we know that H must be abelian because $(xy)^2 = e \implies xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. We can define a bijective mapping $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to H$ such that $f(n, m) = x^n y^m$. f is a homomorphism because

$$f\big((n,m)\big)f\big((a,b)\big) = x^n y^m x^a y^b = x^n x^a y^m y^b = x^{n+a} y^{m+b} = f\big((n,m)(a,b)\big).$$

Thus, $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ □

LEMMA 0.1.3. *All subgroups of cyclic groups are cyclic*

PROOF. Consider the group $\langle a \rangle$ and one of it's subgroups H. Let a^m be an element in H where m is the smallest possible power of a in H (excluding the identity). Now, consider another element $a^n \in H$. $n = qm + r$ where $0 \leq r < m$. $a^n = a^{qm}a^r \implies a^r = a^n\big(a^m\big)^{-q} \in H$. Since a^r belongs in H, $r = 0$. Hence, $H = \langle a^m \rangle$. □

LEMMA 0.1.4. *Given $H \trianglelefteq G$ and $P \in Syl_p(G)$, then $P \cap H \in Syl_p(H)$*

PROOF. $P \cap H$ must be a p-group because it's a subgroup of P, and there must exist a Sylow p-subgroup A of H such that $P \cap H \leq A$. Further, we have $A \leq gPg^{-1} \implies g^{-1}Ag \leq P$, and $A \leq H \implies g^{-1}Ag \leq H$. Thus, $g^{-1}Ag \leq P \cap H$ and $g^{-1}Ag \leq P \cap H \leq A \implies |P \cap H| = |A|$. □

LEMMA 0.1.5. *Given a subgroup H of G such that $|G : H| = p$ where p is the smallest prime that divides G, then H is normal.*

PROOF. Let G act on the cosets of H by left multiplication. Then, we can define the homomorphism $f : G \to S_p$ where $\ker(f)$ is clearly in H (because all elements of the kernal fix H). Now, we know that p divides $|G : \ker(f)|$ and that $|G : \ker(f)|$ divides $p!$. Let $|G : \ker(f)| = pm$. We know m divides $(p-1)!$. If m divides anything other than 1, then we contradict the minimality of p. Thus, $|G : \ker(f)| = p \implies \ker(f) = H$. □

THEOREM 0.1.6 (Fourth Isomorphism Theorem). *Given $G \trianglerighteq K \trianglerighteq H$, $(G/H)/(K/H) \cong G/K$*

PROOF. Let $f : (G/H)/(K/H) \to G/K$ be a map defined such that $f\big(aH(K/H)\big) = aK$. f is well defined because $aH(K/H) = bH(K/H) \implies b^{-1}aH(K/H) = K/H \implies b^{-1}a \in K \implies aK = bK$, and f is a homomorphism because $f\big(aH(K/H)\big)f\big(bH(K/H)\big) = aK \circ bK = abK = f\big(abH(K/H)\big)$. f is injective because $f\big(aH(K/H)\big) = K \implies a \in K \implies aH(K/H) = (K/H) \implies \ker(f) = \{e\}$. Surjectivity holds because $bK = f\big(bH(K/H)\big)$ □

2. Fields

LEMMA 0.1.7. *Suppose a vector space V has a basis of size n. Then, any $n+1$ vectors are linearly dependent.*

PROOF. Let $\{a_1, a_2, \ldots, a_n\}$ be a basis of V. Then, consider the $n+1$ vectors $\{b_1, b_2, \ldots, b_n, b_{n+1}\}$. Since $\{a_1, a_2, \ldots, a_n\}$ spans V, let

$$\begin{aligned} b_1 &= c_{1,1}a_1 + c_{1,2}a_2 + \cdots + c_{1,n}a_n \\ b_2 &= c_{2,1}a_1 + c_{2,2}a_2 + \cdots + c_{2,n}a_n \\ &\vdots \\ b_{n+1} &= c_{n+1,1}a_1 + c_{n+1,2}a_2 + \cdots + c_{n+1,n}a_n \end{aligned}$$

Next, note

$$\begin{aligned} &\implies x_1b_1 + x_2b_2 + \cdots + x_{n+1}b_{n+1} = 0 \\ &\implies (x_1c_{1,1} + x_2c_{2,1} + \cdots + x_{n+1}c_{n+1,1})a_1 + \cdots + (x_1c_{1,n} + x_2c_{2,n} + \cdots + x_{n+1}c_{n+1,n})a_n = 0. \end{aligned}$$

Since $\{a_1, a_2, \ldots, a_n\}$ are linearly independent,

$$\begin{aligned} x_1c_{1,1} + x_2c_{2,1} + \cdots + x_{n+1}c_{n+1,1} &= 0 \\ x_1c_{1,2} + x_2c_{2,2} + \cdots + x_{n+1}c_{n+1,2} &= 0 \\ &\vdots \\ x_1c_{1,n} + x_2c_{2,n} + \cdots + x_{n+1}c_{n+1,n} &= 0 \end{aligned}$$

Notice that this $n \times (n+1)$ system has more variables than equations. Hence, there are infinitely many solutions for $x_1, \ldots, x_{n+1}$ — many of which are when $x_i \neq 0$ (for some $i = 1, \ldots, n+1$). □

LEMMA 0.1.8. *The only solution of the Diophantine equation $a^3 + 2b^3 + 4c^3 - 6abc = 0$ is $a = b = c = 0$.*

PROOF. We prove this by infinite descent. Suppose there exists solutions a, b, c such that either a, b, or c are non-zero. Since a must be even, we set $a = 2a'$. Then,

$$a^3 + 2b^3 + 4c^3 - 6abc = 0 \implies b^3 + 2c^3 + 4(a')^3 - 6a'bc = 0.$$

By the same argument, we can set $b = 2b'$ and then $c = 2c'$ to find that

$$(a')^3 + 2(b')^3 + 4(c')^3 - 6a'b'c' = 0.$$

Notice $\max(|a|, |b|, |c|) > \max(|a'|, |b'|, |c'|)$. By this measurement, we produced a smaller integral solution. We can do this infinitely often, leading to an infinite sequence of smaller integral solutions — an absurd result. □

LEMMA 0.1.9 (Binomial Theorem For Fields). *Let x, y belong to a field F. Then,*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i.$$

PROOF. We proceed by induction on n. Setting $n = 1$, we can see $x + y = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1$. Next, suppose our lemma holds for n. Then,

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n \\ &= \left(\sum_{i=0}^{n}\binom{n}{i}x^{n+1-i}y^i\right) + \left(\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^{i+1}\right) \\ &= x^{n+1} + y^{n+1} + \sum_{i=1}^{n}\binom{n}{i}x^{n+1-i}y^i + \sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}y^{i+1} \\ &= x^{n+1} + y^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}x^{n+1-i}y^i = \sum_{i=0}^{n+1}\binom{n+1}{i}x^{n+1-i}y^i\end{aligned}$$

□

LEMMA 0.1.10. *For all k, $\binom{i}{i} + \binom{i+1}{i} + \cdots + \binom{i+k-1}{i} = \binom{i+k}{i+1}$*

PROOF. We proceed by induction on k. We can see that our lemma holds for $k = 1$. Suppose it was true for $k - 1$. Then,

$$\binom{i+k}{i+1} = \binom{i+k-1}{i} + \binom{i+k-1}{i+1} = \binom{i+k-1}{i} + \binom{i+k-2}{i} + \cdots + \binom{i+1}{i} + \binom{i}{i}.$$

□

LEMMA 0.1.11 (Rational Root Test). *Let $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. Suppose $\frac{a}{b}$ was a root where $\gcd(a, b) = 1$. Then, $b \mid a_n$ and $a \mid a_0$.*

PROOF.

$$p\left(\frac{a}{b}\right) = a_na^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_0b^n = 0$$

(a divides the LHS and the RHS) $\quad a_na^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_1ab^{n-1} = -a_0b^n \implies a \mid a_0$

(b divides the LHS and the RHS) $\quad a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_0b^n = -a_na^n \implies b \mid a_n$

□

LEMMA 0.1.12 (Zorn's Lemma). *Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then, P contains at least one maximal element.*

THEOREM 0.1.13. *Every Vector space has a basis.*

PROOF. In our proof, we employ Zorn's Lemma (Lemma 0.1.12). Now, let V be a vector space. Then, we consider the set of linearly independent subsets of V. In our set, the partial order $\leq$ is defined such that $B_1 \leq B_2 \iff B_1 \subset B_2$. Notice that an upper bound of the chain $B_1 \leq B_2 \leq \ldots$ is $B_1 \cup B_2 \cup \ldots$. Notice that our union must be linearly independent since any subset must be a subset of some B_i. By Zorn's Lemma, we can guarantee the existence of some maximal linearly independent subset $\mathfrak{B}$ of V. $\mathfrak{B}$ must span V for, if it didn't, we contradict the maximality of $\mathfrak{B}$. □

LEMMA 0.1.14. *Call the splitting field of $f \in F[X]$ over F K. Given f has no repeated roots over K, K/F is seperable.*

PROOF. Theorem 3.5 of [**Con14**]. □

LEMMA 0.1.15. *Consider $g, h \in \mathbb{Z}[X]$ such that h and g have leading coefficient 1 and $h \mid g$ in $\mathbb{C}[X]$. Then, $h \mid g$ in $\mathbb{Z}[X]$.*

PROOF. Let $\deg g = m$ and $\deg h = n$. We proceed by induction on $m - n$. Suppose $m = n$. Then, $g(x) = h(x)$. Now, suppose $m > n$. Assume our result holds for all $0 \leq i < m - n$. Then, notice $h(x)$ divides $g(x) - x^{m-n}h(x)$ and $x^{m-n}h(x)$ over $\mathbb{Z}[X]$ by the inductive hypothesis. h must then divide g over $\mathbb{Z}[X]$. □

LEMMA 0.1.16. *Let $\{d_i\}_{i=1}^m$ be the set of m divisors of n. Then,*

$$\phi(d_1) + \phi(d_2) + \cdots + \phi(d_m) = n.$$

PROOF. Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where $p_1, p_2, \dots, p_k$ are primes. Then,

$$\begin{aligned}
&= \phi(d_1) + \phi(d_2) + \cdots + \phi(d_m) \\
&= \left(\phi(1) + \phi(p_1) + \phi\left(p_1^2\right) + \cdots + \phi\left(p_1^{e_1}\right)\right) \times \cdots \times \left(\phi(1) + \phi(p_k) + \phi\left(p_k^2\right) + \cdots + \phi\left(p_k^{e_k}\right)\right) \\
&= \left(1 + p_1 - 1 + p_1^2 - p_1 + \cdots + p_1^{e_1} - p_1^{e_1 - 1}\right) \times \cdots \times \left(1 + p_k - 1 + p_k^2 - p_k + \cdots + p_k^{e_k} - p_k^{e_k - 1}\right) \\
&= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = n
\end{aligned}$$

□

LEMMA 0.1.17. *In $\mathbb{F}_p[X]$ (p is prime), $g(x^p) = (g(x))^p$.*

PROOF. Note $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{F}_p$ by Fermat's Little Theorem and $(x+y)^p \equiv x^p + y^p \pmod{p}$ for indeterminate x and y by the Binomial Theorem (Lemma 0.1.9). Our result then follows. □

LEMMA 0.1.18 (The Galois Group acts transitively on the roots). *Let x and y be roots of the separable, minimal polynomial $f \in F[X]$. Call the splitting field of f over F K. Then, there exists $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(x) = y$.*

PROOF. Consider the polynomial

$$g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \sigma(x)).$$

Notice that it is invariant under the elements of $\mathrm{Gal}(K/F)$ and, hence, belongs in $F[X]$. Then, $f \mid g \implies g(y) = 0$. I.e. there exists σ such that $\sigma(x) = y$. □

LEMMA 0.1.19. *Let $\sigma : F \to F'$ be an isomorphism of fields. Let $p \in F[X]$, and let $p' \in F'[X]$ be the polynomial obtained by applying σ on the coefficients of p. Call the K the splitting field of p over F and K' that of p' over F'. Then, there exists an isomorphsim $\tau : K \to K'$ such that τ restricts to σ. I.e. $\forall x \in F$, $\tau(x) = \sigma(x)$.*

PROOF. 13.1, Theorem 8 of [**DF04**]. □

LEMMA 0.1.20. *For transcendental x, $F(x)$ consists of elements of the form $f(x) = \frac{g(x)}{h(x)}$ where $h, g \in F[X]$ and. Under function composition, the only elements with inverses in $F(x)$ are those of the form*

$$\frac{ax + b}{cx + d}$$

where $ad \neq bc$.

PROOF. For $f(x) = \frac{g(x)}{h(x)} \in F(x)$ (where g and h are relatively prime), suppose it has an inverse under composition in $F(x)$. Denote its inverse f^{-1}. Define $\deg f$ as

$$\deg f = \begin{cases} \deg g & \deg g \geq \deg h \\ \deg h & \deg h > \deg g. \end{cases}$$

Notice that, when rational functions are composed in $F(x)$, their degrees are multiplied. Hence, $\deg f \circ f^{-1} = 1 \implies \deg f = \deg f^{-1} = 1$. It follows that there exists $a, b, c, d \in F$ such that

$$f(x) = \frac{ax+b}{cx+d}$$
$$f^{-1}(x) = \frac{b-dy}{cy-a} = \frac{-b(\frac{d}{b}y - 1)}{a(\frac{c}{a}y - 1)}$$

$f^{-1}(x) \in F(x) \iff c/a \neq d/b \iff ad \neq bc.$ □

LEMMA 0.1.21 (Properties of Quadratic Residues and the Legendre Symbol). *For odd prime p, let $x \in \mathbb{F}_p$ ($x \not\equiv 0 \pmod p$) be a quadratic residue if and only if there exists y such that $y^2 \equiv x \pmod p$.*

(1) In $\mathbb{F}_p$, there are $\frac{p-1}{2}$ quadratic residues.
(2) In $\mathbb{F}_p$, -1 is a quadratic residue if and only if $p \equiv 1 \pmod 4$.
(3) For integer $m \in [1, p-1]$, $\left(\frac{1(1-m)}{p}\right) + \left(\frac{2(2-m)}{p}\right) + \cdots + \left(\frac{(p-1)(p-1-m)}{p}\right) = -1$.

PROOF.

(1) Notice that $x^2 - a^2 \equiv 0 \pmod p$ has precisely two solutions — $\{a, -a\}$. It follows that our full set of quadratic residues is $\{1, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$.
(2) Suppose $p \equiv 1 \pmod 4$. Then, by Wilson's Theorem,

$$-1 \equiv (p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \times (-1)^{\frac{p-1}{2}} \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p.$$

Now, suppose there exists x such that $x^2 \equiv -1 \pmod p$. Then, $x^4 \equiv 1 \pmod p$, and, hence, by Lagrange's Theorem, $p \equiv 1 \pmod 4$.
(3) Notice that, since $\left(\frac{i}{p}\right) = \left(\frac{i^{-1}}{p}\right)$,

$$\sum_{i=1}^{p-1} \left(\frac{i(i-m)}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{(1-mi^{-1})}{p}\right) = \sum_{j \in \mathbb{F}_p / \{1\}} \left(\frac{j}{p}\right) = \sum_{j \in \mathbb{F}_p} \left(\frac{j}{p}\right) - \left(\frac{1}{p}\right) = -1.$$

□

LEMMA 0.1.22. *Consider a subgroup $G \leq S_n$. If G is 2-transitive and has a transposition (a, b), $G = S_n$*

PROOF. Consider an arbitrary transposition (x, y). As G is 2-transitive, let $f \in G$ be an element for which $f(x) = a$ and $f(y) = b$. Then, $f(a, b)f^{-1} = (f(a), f(b)) = (x, y) \in G$. As S_n is generated by the transpositions, $G = S_n$. □

LEMMA 0.1.23. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial. For prime p, let $\overline{f}$ be the reducation of f modulo p. Call the splitting field of f over $\mathbb{Q}$ K and that of $\overline{f}$ over $\mathbb{F}_p$ $\overline{K}$. Then,* $\mathrm{Gal}(\overline{K}/\mathbb{F}_p) \leq \mathrm{Gal}(K/\mathbb{Q})$.

PROOF. Ch VII, Theorem 2.9 of [**Lan02**]. □

LEMMA 0.1.24. *F is a field if and only if $F[x]$ is a Principle Ideal Domain.*

PROOF. Suppose F is a field. Consider an ideal $I \subseteq F[x]$. If $I = \{0\}$, $I = (0)$. Otherwise, choose non-zero $f \in I$ with smallest degree. For $g \in I$, we employ the division algorithm to note

$$g(x) = q(x)f(x) + r(x) \implies r(x) = g(x) - q(x)f(x) \in I \implies r(x) = 0.$$

Hence, $I = (f)$. Now, suppose $F[X]$ is a PID. Choose non-zero $a \in F$. Then, $(a, x) = (f)$ for some $f \in F[x]$. As $a \in (f)$, $\deg f = 0$. As $x \in (f)$, there exists $f^{-1} \in F$ such that $ff^{-1}x = x \implies f \in F^\times$. Hence, $(f) = F[X]$, and there exists $a^{-1}, q \in F$ such that $a^{-1}a + qx = 1 \implies a^{-1}a = 1 \implies a \in F^\times$. □

LEMMA 0.1.25. *For prime p and $f \in \mathbb{Z}[x]$, denote $\overline{f}$ as the reduction of f modulo p. Then,*

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(\overline{f}(x))}.$$

PROOF. Let $\phi : \mathbb{Z}/p\mathbb{Z}[x] \to \mathbb{Z}[x]/(p, f(x))$ be defined such that $\phi(g) = r + (p, f(x)) \iff g(x) = q(x)\overline{f}(x) + r(x)$ where $\deg r < \text{def } \overline{f}$. Noting that ϕ is a homomorphism, we proceed to show $\text{im}(\phi) = \mathbb{Z}[x]/(p, f(x))$ and $\ker(\phi) = (\overline{f}(x))$. Since

$$h(x) \equiv \overline{h}(x) \pmod p \implies h(x) - \overline{h}(x) \in (p) \implies h(x) - \overline{h}(x) \in (p, f(x)) \tag{1}$$

$$\overline{h}(x) = q(x)\overline{f}(x) + r(x) \implies \overline{h}(x) - r(x) \in (p, f(x)), \tag{2}$$

ϕ is surjective. Suppose $\phi(g(x)) = (f(x), p)$ and $g(x) = q(x)\overline{f}(x) + r(x)$. Then, $r(x) = af(x) + bp = \overline{a}\overline{f}(x)$ (as r is reduced mod p) and $g(x) = (\overline{a} + q(x))\overline{f}(x) \in (\overline{f}(x))$. I.e. $\ker(\phi) = (\overline{f}(x))$. □

3. Rings & Geometry

LEMMA 0.1.26. *If a ring R is a Unique Factorization Domain, then $R[x]$ is a Unique Factorization Domain.*

PROOF. Section 9.3, Theorem 7 of [DF04] □

LEMMA 0.1.27. *For a field F and irreducible, degree n polynomial $f \in F[x]$ with root α, $F[x]/(f) \cong F(\alpha)$.*

PROOF. Consider the map $\phi : F[x] \to F(\alpha)$ defined by evaluation at α. Noting that

$$\phi(f(x)g(x)) = f(\alpha)g(\alpha) = \phi(f(x))\phi(g(x)) \tag{3}$$

$$\phi(f(x) + g(x)) = f(\alpha) + g(\alpha) = \phi(f(x)) + \phi(g(x)) \tag{4}$$

$$\phi(1) = 1 \tag{5}$$

$$\phi(f(x)) = a_{n-1}\alpha^{n-1} + \cdots + a_0 \implies f(x) = a_{n-1}x^{n-1} + \cdots + a_0 \tag{6}$$

ϕ is a surjective homomorphsim. Since f is minimal, $g(\alpha) = 0 \iff f \mid g$. I.e. $\ker(\phi) = (f)$, and, hence, the desired result follows from the first isomorphism theorem. □

LEMMA 0.1.28 (Sum of Squares). *In a ring R, the product of a sum of squares is a sum of squares.*

PROOF. Let $a, b, c, d \in R$. Then,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

LEMMA 0.1.29. *In $\mathbb{R}$, the intersection of closed intervals is either a closed interval, a point, or the empty set.*

PROOF. If $[a, b] \subseteq [c, d]$ or $[c, d] \subseteq [a, b]$, the result is apparent. If $a \le c \le b \le d$, $[a, b] \cap [c, d] = [c, b]$. If $a \le b = c \le d$, $[a, b] \cap [c, d] = \{b\}$, and $a \le b < c \le d$, $[a, b] \cap [c, d] = \varnothing$. □

LEMMA 0.1.30. *Let R be integrally closed. Then, $S^{-1}R$ is integrally closed for any multiplicative subset S of R.*

PROOF. Consider $\alpha \in \text{Frac}(R)$ (which is the same as $\text{Frac}(S^{-1}R)$) for which there exists monic $f \in S^{-1}R[x]$ such that

$$f(\alpha) = \alpha^n + \frac{r_{n-1}}{s_{n-1}}\alpha^{n-1} + \cdots + \frac{r_0}{s_0} = 0.$$

Since $\alpha s_{n-1} \cdots s_0$ is a root of the monic polynomial

$$(s_{n-1} \cdots s_0)^n f\left(\frac{x}{s_{n-1} \cdots s_0}\right)$$

in $R[x]$, we use that R is integrally closed to conclude

$$\alpha s_{n-1} \cdots s_0 \in R \implies \alpha = \frac{\alpha s_{n-1} \cdots s_0}{s_{n-1} \cdots s_0} \in S^{-1}R.$$

□

LEMMA 0.1.31. *Let R be a Principle Ideal Domain. Then, R is integrally closed.*

PROOF. We begin by noting that all PIDs are UFDs and, hence, GCD domains. Then, we employ what is essentially the *Rational Root Theorem* to note if $\frac{a}{b} \in \text{Frac}(R)$ where $\gcd(a, b) \in R^\times$, then

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0 \qquad (a_i \in R \text{ for all } i = 0, \ldots, n-1)$$

implies $b \mid a^n$. b must then be a unit, and, hence, $\frac{a}{b} = ab^{-1} \in R$. □

LEMMA 0.1.32. *Let $f(x, y) = x^i - y^j$, where $\gcd(i, j) = 1$. Then, f is irreducible.*

PROOF. Suppose $f(x, y) = g(x, y)h(x, y)$. Then, $f(t^j, t^i) = 0$ implies $g(t^j, t^i)$ or $h(t^j, t^i)$ is the zero polynomial. WLOG,

$$g(x, y) = \sum_{m+n} a_{m,n} x^m y^n \tag{7}$$

$$0 = \sum_{s=jm+in} a_{m,n}. \tag{8}$$

Suppose there exists m', n' such that

$$jm + in = jm' + n' \implies j(m - m') = i(n' - n).$$

Since $\gcd(i, j) = 1$, $m \equiv m' \pmod{i}$ and $n \equiv n' \pmod{j}$. Assuming $i > j$, $m, m' \in \{0, \ldots, m-1\}$ and $m = m'$. It follows $n = n'$. We may apply a similar argument when $j > i$. Thus, $g(x, y)$ is the zero polynomial (contradiction!) □

Part 1

Group Theory

CHAPTER 1.1

Introduction To Groups

Problem 1. Check that the symmetric group is a group, i.e. that it satisfies all the group properties

Solution 1.

- Consider two elements g and h in S_n. Because both elements run from and to $\{1, 2, 3, \ldots, n\}$, $g \circ h$ also runs from and to $\{1, 2, 3, \ldots, n\}$, and, because g and h are bijections, $g \circ h$ is also a bijection. Thus, $g \circ h \in S_n$
- Consider the element $I \in S_n$ such that for all a $\in \{1, 2, 3, \ldots, n\}$, $I(a) = a$. This element is the identity
- Function composition is associative because $f \circ (g \circ h)(a) = f(g(h(a))) = (f \circ g) \circ h(a)$
- The elements of a symmetric group are bijective functions from and to $\{1, 2, 3, \ldots, n\}$. Since these functions are bijective and run from and to the same set, we know the inverse of every element must belong S_n

Problem 2. If $g, h \in G$, show that $(gh)^{-1} = h^{-1}g^{-1}$

Solution 2. $(gh)(gh)^{-1} = e \implies h^{-1}g^{-1}gh(gh)^{-1} = h^{-1}g^{-1} \implies (gh)^{-1} = h^{-1}g^{-1}$

Problem 3. Show that rigid motions have inverses; that is, if f is a rigid motion, then there is a rigid motion g so that $g \circ f$ and $f \circ g$ are both the identities

Solution 3. There are four possible rigid motions - rotations, translations, reflections, and glide reflections - that each have their own inverse.

- The inverse of a translation by vector $\overrightarrow{A}$ is a translation by vector $-\overrightarrow{A}$
- The inverse of a rotation by angle θ with point P as the center is a rotations about point P by angle $-\theta$
- The inverse of a reflection across any line is itself
- The inverse of a glide reflections across any line and by any vector $\overrightarrow{A}$ is another glide reflection across the same line and by the vector $-\overrightarrow{A}$

Problem 4. Explain why function composition is associative

Solution 4. Note that this is essentially the same as what was presented in Problem One but with more detail

$$\begin{aligned}[f \circ (g \circ h)](a) &= f((g \circ h)(a)) \\ &= f(g(h(a))) \\ &= [f \circ g](h(a)) \\ &= ([f \circ g] \circ h)(a)\end{aligned}$$

Problem 5. Explain how to represent any reflection in D_n using just ρ and τ

Solution 5. Begin by noting that the elements of D_n are either rotations or reflections about the lines of symmetry of an n-gon. The rotations are obviously all powers of ρ. The reflections are as follows:

For an odd n, each line of reflection passes through a vertex. Thus, one could simply rotate the object such that it (the line of reflection) is directly on the line τ reflects across, reflect it, and, then, rotate it back. More specifically, if we consider a regular polygon with one vertex aligned on $(0, 1)$ and label each vertex from 0 (This would be the vertex on $(0, 1)$) to $n-1$ clockwise, then a reflection across the line of symmetry passing through vertex m would be $\rho^{-m}\tau\rho^m = \tau\rho^{2m}$

For an even n, reflecting about the lines passing through the vertices would be the exact same, but reflecting about those passing through the mid-points of the sides differ. Once again, consider a regular polygon with one vertex aligned on $(0, 1)$ and label the mid points of each side from 1 to n clockwise. Then, a reflection about the line passing through mid point m is simply $\tau\rho^m$

Problem 6. Given an element $\sigma \in S_n$, written in cycle notation, how do you determine its order easily?

Solution 6. Consider the element $f \in S_n$, written below in cyclic notation:

$$f = a_1 \to a_2 \to a_3 \to \cdots \to a_k \to \cdots \to a_n$$

Below are the partial cycles of f^m for a fixed $1 \leq k \leq n$, presented to demonstrate a trend.

$$\begin{aligned} f^1 &= \cdots a_k \to a_{k+1} \cdots \\ f^2 &= \cdots a_k \to a_{k+2} \cdots \\ f^3 &= \cdots a_k \to a_{k+3} \cdots \\ &\vdots \\ f^n &= \cdots a_k \to a_{k+n} \cdots \end{aligned}$$

From the definition of f, the partial cycle $a_k \to a_{k+1}$ already exists in f^1. Now, suppose the partial cycle $a_k \to a_{k+m-1}$ exists in f^{m-1}. Then, upon multiplying f^{m-1} with f, the partial cycle becomes $a_k \to a_{k+m}$. Hence, for every positive integer m, $f^m = \cdots a_k \to a_{k+m} \cdots$

Note that the partial cycle $a_p \to a_q$ is equivalent to $a_{p \mod n} \to a_{q \mod n}$ for all $p, q \in \mathbb{Z}$ and $p, q \geq 1$

Thus,

$$f^n = \cdots a_k \to a_{k+n} \cdots = \cdots a_k \to a_k \cdots = e$$

I.e. the order of function consisting of a single cycle is the size of said cycle

For an element $g \in S_n$ that isn't a single cycle, we may consider the representation of g as the product of multiple disjoint cycles. Let $g = a_1 a_2 a_3 \dots a_n$. Since the cycles are disjoint, we know they commute, and, hence, $g^m = a_1^m a_2^m a_3^m \dots a_n^m$. It's now easy to see why $m = LCM(|a_1|, |a_2|, |a_3|, \dots, |a_n|)$ is the smallest such m for which $g^m = e$

Problem 7. Let n be a positive integer, and let $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$. Show that μ_n is a group under multiplication. How many elements does it have?

Solution 7.

- 1 is the identity element (Note that for all n, 1 is a root of $z^n - 1$)
- If α is an element of μ_n, then $\alpha^{-1} = \frac{1}{\alpha}$, and, since $\left(\frac{1}{\alpha}\right)^n = \frac{1}{\alpha^n} = 1$, α^{-1} is clearly an element of μ_n
- Given two elements α and β in μ_n, $\alpha \times \beta$ is also an element of μ_n since $(\alpha \times \beta)^n = \alpha^n \times \beta^n = 1$
- Multiplication is associative

since $\frac{d}{dz}(z^n - 1) \neq 0$ for all $z \in \mu_n$, we know we have no repeated roots, and, hence, μ_n has exactly n elements.

Problem 8. For which elements $\sigma \in S_n$ is σ equal to its inverse σ^{-1}?

Solution 8.

$$\sigma = \sigma^{-1} \iff \sigma^2 = e$$

Clearly, any function with an order of two is equivalent to its inverse. Further, from the deductions of Problem Seven, we know that these functions must be cycles of size of two or the product of disjoint cycles of size two.

Problem 9. Let X be the shape formed by taking two regular tetrahedra of the same size and gluing them together along a common face. How many symmetries does the resulting figure have?

Solution 9. Consider the triangular face shared by the two tetrahedra. The symmetries of this face would also be the symmetries of shape X. Then, one could also reflect shape X about the plane face X lies on and apply the same symmetries as before. Hence, the number of symmetries is $2 \times |D_3| = 12$.

Alternatively, one could label the five different vertices of shape X and find the different permutations of said vertices such that the relative distance between each vertex is maintained. Upon doing so, one would find that there are $2 \times 3 \times 2 = 12$ different possible symmetries.

Problem 10. What are all the rigid motions f such that $f(0,0) = (1,0)$?

Solution 10.

- The rigid motion e defined such that $e(P) = P$
- Any rotation about point (0,0)
- Any reflection about a line passing through (0,0)

Problem 11. What are all the rigid motions f such that $f(0,0) = (1,0)$?

Solution 11.

- A translation by the vector $\hat{\imath}$
- A rotation with centre $(0.5, k)$ and angle $\theta = 2\tan^{-1}(\frac{1}{2k})$
- A reflection about line $x = 0.5$

When it comes to the glide reflections, the set of those that send $(0,0)$ to $(1,0)$ can be described as follows. First consider a circle with center $(0.5, 0)$ and radius $\frac{1}{2}$. On said circle, pick any point α (other than $(0,0)$), and we can draw a segment connecting $(0,0)$ to α. The perpendicular bisector of this segment passes through $(0.5, 0)$, and, upon reflecting $(0,0)$ by this line, we have α. The line passing through α and $(0,1)$ is parallel to our line of reflection so we can simply translate α to $(0,1)$. This is our glide reflection.

Problem 12. $\mathbb{Z}/n\mathbb{Z}$ does not form a group under multiplication. However, it is possible to make a subset of the elements of $\mathbb{Z}/n\mathbb{Z}$ into a group under multiplication. What is the largest possible subset for which

this works?

Solution 12. The group of integers modulo n under multiplication shall be defined such that every element of the group is relatively prime to n. Associativity follows from multiplication, and the group is closed under multiplication because if a and b are relatively prime to n, then ab must be relatively prime to n. The identity element is obviously 1.

Inverses must also exists because, since a is relatively prime to n,

$$xa + mn = 1 \iff xa = 1 + n(-m) \iff xa \equiv 1 \mod n \iff x = a^{-1}$$

and for the same reason, this is largest possible set for this to work.

Problem 13. Suppose that τ and ρ are the standard reflection and rotation (respectively) in the dihedral group D_6. Write $\rho^4\tau\rho\tau\rho^3$ in the form $\tau^a\rho^b$, where $0 \leq a \leq 1$ and $0 \leq b \leq 5$.

Solution 13. $\rho^4\tau\rho\tau\rho^3 = \tau\tau\rho^4\rho^{-1}\rho^3 = \tau^2\rho^6 = e$

Problem 14. Let $\sigma, \tau \in S_6$ be the elements

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 6 & 2 & 3 \end{pmatrix} \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 4 & 2 & 5 \end{pmatrix}$$

Write the elements σ and τ in cycle notation. Compute $\sigma\tau$ and $\tau\sigma$. Are they equal?

Solution 14.

$$\sigma = (146352)$$
$$\tau = (1652)$$
$$\sigma\tau = (135)\ (246)$$
$$\tau\sigma = (145)\ (326)$$

Clearly, $\sigma\tau \neq \tau\sigma$.

Problem 15. We say that a group G is cyclic if there is some element $g \in G$ so that for each $h \in G$, there is some integer n so that $g^n = h$. (In other words, every element is a power of g.) Show that every cyclic group is abelian. Can you find an abelian group which is not cyclic?

Solution 15.

(By the commutativity of addition) $$g^{n_1} \circ g^{n_2} = g^{n_1+n_2} = g^{n_2+n_1} = g^{n_2} \circ g^{n_1}$$

As for a non-cyclic abelian group, consider the subgroup $\{e, \rho^2, \tau, \tau\rho^2\}$ of D_4

Problem 16. Show that a dihedral group can be generated by two elements, each of which is its own inverse.

Solution 16. Consider the elements $\rho\tau$ and τ. $\tau = \tau^{-1}$ (it's a reflection) and $(\rho\tau)^{-1} = \tau^{-1}\rho^{-1} = \tau\rho^{-1} = \rho\tau$. Further, since $\rho\tau\tau = \rho$, we may conclude both $\rho\tau$ and τ are generators of D_n.

Problem 17. Show that every group of order 4 is abelian.

Solution 17. Let's assume there exists a group of order 4 that isn't abelian. I.e. in a group G, there exists distinct, non-identity elements a and b such that $ab \neq ba$. Then, we know $\{e, a, b, ab, ba\} \subset G$, which implies $|G| > 4$ (contradiction!)

Problem 18. Let G be a finite abelian group with elements $g_1, \ldots, g_n$. Show that the product $g_1 g_2 \ldots g_n$ is equal to the product of the elements of order 2. Deduce Wilson's Theorem, which says that if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Solution 18. The elements of order two and one are their own inverse. For elements of a greater order, there exists an inverse distinct from the element itself. Begin by seperating the product of all elements in G into the product of elements of order 2 and 1 and the product of elements of a greater order. Suppose $g_1 g_2 \ldots g_k$ is the product of elements of order 2 and 1 while $g_{k+1} g_{k+2} \ldots g_n$ is the product of the other elements. Then,

$$g_1 g_2 \ldots g_n = (g_1 g_2 \ldots g_k)(g_{k+1} g_{k+2} \ldots g_n) = (g_1 g_2 \ldots g_k)$$

because for every g_i $(k+1 \leq i \leq n)$, there exists g_j $(k+1 \leq j \leq n)$ such that $(g_i)^{-1} = g_j$

Consider the group $(\mathbb{Z}/p\mathbb{Z})^\times$ (Note that this is a group because p is prime). $x^2 \equiv 1 \mod p \implies p|(x+1)$ or $p|(x-1) \implies x \equiv 1 \mod p$ or $x \equiv -1 \mod p$. We may then conclude that the product of the elements of $\mathbb{Z}/p\mathbb{Z}$ is $1 \times -1 \equiv -1 \mod p$. I.e.

$$(p-1)! \equiv -1 \mod p$$

CHAPTER 1.2

Structure Of Groups

Exercise 1. Can you list all subgroups of D_4?

Solution.

- $\{e\}$
- $\{e, \rho^2\}$, $\{e, \tau\}$, $\{e, \tau\rho\}$, $\{e, \tau\rho^2\}$, $\{e, \tau\rho^3\}$
- $\{e, \rho, \rho^2, \rho^3\}$, $\{e, \rho^2, \tau, \tau\rho^2\}$
- $\{e, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}$

Exercise 2. Consider the groups G and H. Check that $G \times H$ inherits associativity from G and H.

Solution. $\Big((g_1, h_1)(g_2, h_2)\Big)(g_3, h_3) = (g_1g_2g_3, h_1h_2h_3) = (g_1, h_1)\Big((g_2, h_2)(g_3, h_3)\Big)$

Exercise 3. For a non-abelian group G, why is the map $f : G \to G$ where $f(g) = g^{-1}$ not an automorphism?

Solution. Assume f is a homomorphism and consider the arbitrary elements a, b in G. $f(ab) = f(a)f(b) = a^{-1}b^{-1}$ and $f(ab) = (ab)^{-1} = b^{-1}a^{-1}$. Hence, $a^{-1}b^{-1} = b^{-1}a^{-1} \implies ba = ab$. G is, therefore, abelian.

Problem 1. Show that if G and H are finite groups, and $G \cong H$, then $|G| = |H|$. Find an example to show that the converse is false.

Solution 1. Since $G \cong H$, there exists a bijective map $f : G \to H$ (f is also a homomorphism but that doesn't matter). Thus, $|G| = |H|$. The converse doesn't hold because $|D_6| = |\mathbb{Z}/12\mathbb{Z}| = 12$ but D_6 isn't isomorphic to $\mathbb{Z}/12\mathbb{Z}$ (D_6 isn't abelian but $\mathbb{Z}/12\mathbb{Z}$ is).

Problem 2. Show that $G \times H \cong H \times G$.

Solution 2. The isomorphism $f : G \times H \to H \times G$ is defined as follows:

$$f\Big((g, h)\Big) = (h, g)$$

f is clearly a homomorphism because

$$f\Big((g_1, h_1)(g_2, h_2)\Big) = f\Big((g_1g_2, h_1h_2)\Big) = (h_1h_2, g_1g_2)$$

and

$$f\Big((g_1, h_1)\Big)f\Big((g_2, h_2)\Big) = (h_1, g_1)(h_2, g_2) = (h_1h_2, g_1g_2).$$

Further, since the function simply swaps g and h, it's clearly bijective.

Problem 3. Show that if $H, K \leq G$, then $H \cap K \leq G$. Show that $H \cup K$ is not necessarily a subgroup of G.

Solution 3. Suppose $a, b \in H \cap K$. Then, $a, b \in H$ and $a, b \in K$, and, hence, $ab \in H$ and $ab \in K$ (by the closure of H and K), which implies $ab \in H \cap K$. Further, $a^{-1} \in H$ and $a^{-1} \in K$, and, hence, $a^{-1} \in H \cap K$. Thus, $H \cap K$ is a subgroup of G. Now, consider H and K such that H isn't a subset of K (and vice versa). Then, there exists $a \in H$ such that $a \notin K$ and $b \in K$ such that $b \notin H$. $ab \in H \cup K$ implies $ab \in H$ or $ab \in K$. Without loss of generality assume $ab \in H$. Then, $a^{-1}(ab) = b \in H$ (contradiction!). Thus, for our chosen H and K, $H \cup K$ can't be closed. As an example of such H and K, consider the subgroups $\{e, \rho^2\}$ and $\{e, \tau\}$ of D_4

Problem 4. When is the function $f : G \to G$ given by $f(g) = g^2$ a homomorphism?

Solution 4. $f(g_1g_2) = g_1g_2g_1g_2 = g_1^2g_2^2 = f(g_1)f(g_2)$ if and only if $g_2g_1 = g_1g_2$. Thus, G must be abelian.

Problem 5. We showed that if $f : G \to H$ is a homomorphism and $g \in G$ has order n, then $f(g) \in H$ has order $\leq n$. Show that the order of $f(g)$ divides n.

Solution 5. Let m be the order of $f(g)$ and $n = qm + r$ (where $0 \leq r < m$). Then,

$$f(g^n) = \big(f(g)\big)^n = \big(f(g)\big)^{qm}\big(f(g)\big)^r = e \implies r = 0$$

Problem 6. Is every subgroup of $G_1 \times G_2$ necessarily of the form $H_1 \times H_2$, where $H_1 \leq G_1$ and $H_2 \leq G_2$? Give a proof or find a counterexample.

Solution 6. Consider the group $\mathbb{Z} \times \mathbb{Z}$ and its subgroup $S = \{(x, x) : x \in \mathbb{Z}\}$. Here, if S could be broken into $H_1 \times H_2$ (where $H_1, H_2 \leq \mathbb{Z}$), $H_1, H_2 = \mathbb{Z}$, but we can see that $S \neq \mathbb{Z} \times \mathbb{Z}$.

Problem 7. Let p be a prime, and let $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. How many subgroups of order p does G have? What if G is a product of n copies of $\mathbb{Z}/p\mathbb{Z}$, for $n \geq 2$?

Solution 7. For our solution, we'll skip straight to the generalization. In $(\mathbb{Z}/p\mathbb{Z})^n$, there are $p^n - 1$ elements of order p, and for every group generated by one of these elements, there exists $p - 2$ other elements that generate the same group (by Lemma 0.1.1). Thus, there exists

$$\frac{p^n - 1}{p - 1} = \sum_{i=0}^{n-1} p^i$$

subgroups of order p

Problem 8. Let $f : G \to H$ be a homomorphism. Show that $\ker(f) \leq G$ and $\mathrm{im}(f) \leq H$. (In other words, the kernel and image are subgroups are G and H, respectively.)

Solution 8. Let $g_1, g_2 \in \ker(f)$. Then $f(g_1g_2) = f(g_1)f(g_2) = e_H$, which implies $g_1g_2 \in \ker(f)$. Further, $f(g_1^{-1}) = (f(g_1))^{-1} = e_H$ and, hence, $g_1^{-1} \in \ker(f)$. Thus, $\ker(f) \leq G$. Let $h_1, h_2 \in \mathrm{im}(f)$. Then, there exists g_1 and g_2 such that $f(g_1) = h_1$ and $f(g_2) = h_2$. $f(g_1g_2) = f(g_1)f(g_2) = h_1h_2$ and, hence, $h_1h_2 \in \mathrm{im}(f)$. Further, $f(g_1^{-1}) = (f(g_1))^{-1} = h_1^{-1}$ and, hence, $h_1^{-1} \in \mathrm{im}(f)$. Thus, $\mathrm{im}(f) \leq H$.

Problem 9. Let $f : G \to H$ be a homomorphism of groups. Prove that

(1) f is injective if and only if $\ker(f) = \{e_G\}$
(2) f is surjective if and only if $\text{im}(f) = H$

Solution 9. To prove claim 1, we begin by considering the contrapositve. The contrapositve holds from the definition of injectivity (if $\ker(f)$ is non-trivial, then there exists distinct $a, b \in G$ such that $f(a) = e_H = f(b)$. I.e. f is not injective). We now consider the inverse. If f is not injective, then there exists distinct a and b such that $f(a) = f(b) \implies f(a)\left(f(b)\right)^{-1} = e_H \implies f(ab^{-1}) = e_H$. Since a and b are distinct, $ab^{-1} \neq e$ and, thus, $|\ker(f)| \geq 2$. Hence, claim one holds true. Claim 2 holds true from the definition of surjectivity.

Problem 10. Prove that a homomorphism $f : G \to H$ is an isomorphism if and only if there exists a homomorphism $f^{-1} : H \to G$ with $\left(f^{-1} \circ f\right)(g) = g$ for all $g \in G$, and $\left(f \circ f^{-1}\right)(h) = h$ for all $h \in H$.

Solution 10. Let f be an isomorphism. Because f is a bijective map, we know there exists an inverse, bijective map f^{-1} that must be a homomorphism because $f^{-1}\left(f(a)f(b)\right) = f^{-1}\left(f(ab)\right) = ab = f^{-1}\left(f(a)\right)f^{-1}\left(f(b)\right)$. Now, suppose for a map f, there exists an inverse f^{-1} that is a homomorphism. The existence of an inverse guarantees that f is bijective and, through the same argument above, we may conclude f is a homomorphism.

Problem 11. Show that $\text{Aut}(G)$ is a group. Show that $\text{Inn}(G) \leq \text{Aut}(G)$.

Solution 11.

- Mapping composition is associative, and, for the same reason, the composition of automorphisms is as well
- Let $f, g \in \text{Aut}(G)$. Then, $f \circ g$ is an automorphsim because $g\left(f(g_1 g_2)\right) = g\left(f(g_1)f(g_2)\right) = g\left(f(g_1)\right)g\left(f(g_2)\right)$ and because the composition of bijective functions is bijective.
- The identity element is the automorphism f, defined such that $f(g) = g$ for all $g \in G$
- Since all automorphisms are isomorphisms, there must be an inverse for every element by **Problem 10.**

$\text{Inn}(G)$ is a subset of $\text{Aut}(G)$. Thus, we need only show that closure holds and inverses exists to prove $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.

- $\left(\varphi_{h_1}\varphi_{h_2}\right)(g) = h_1^{-1}h_2^{-1}gh_2h_1 = (h_2h_1)^{-1}g(h_2h_1) = \varphi_{h_2h_1}(g)$ (closure)
- $(\varphi_{h_1})^{-1}(g) = h_1gh_1^{-1} = \varphi_{h_1^{-1}}(g)$ (inverse)

Problem 12. If $\sigma \in S_n$ is a permutation, then its cycle type is the sequence $(a_1, a_2, \ldots, a_n)$, where a_i is the number of cycles of length i in the cycle decomposition of σ (written in cycle notation).

(a) Let σ be the i-cycle $(x_1, \ldots, x_i)$, written in cycle notation. For any $\tau \in S_n$, show that $\tau\sigma\tau^{-1} = (\tau(x_1), \ldots, \tau(x_i))$.
(b) Show that for any $\sigma, \tau \in S_n$, σ and $\tau\sigma\tau^{-1}$ have the same cycle type.
(c) Conclude that if ϕ is an automorphism of S_n, and there is some σ such that σ and $\phi(\sigma)$ have different cycle types, then ϕ is an outer automorphism.

Solution 12.

(a) Consider an object x_m such that $\sigma(x_m) = x_{m+1}$. Then, $(\tau\sigma\tau^{-1})(\tau(x_m)) = \tau(\sigma(\tau^{-1}(\tau(x_m)))) = \tau(x_{m+1})$. Similarly, if we consider an object j such that $\sigma(j) = j$, then $(\tau\sigma\tau^{-1})(\tau(j)) = \tau(\sigma(\tau^{-1}(\tau(j)))) = \tau(j)$. Hence, $\tau\sigma\tau^{-1} = (\tau(x_1), \tau(x_2), \tau(x_3), \ldots, \tau(x_i))$
(b) We know that σ has one i-cycle and $n - i$ one cycles, and, from **(a)**, we know that $\tau\sigma\tau^{-1}$ also has one i-cycle and $n - i$ one cycles. Thus, the two permutations must have the same cycle type.
(c) **(b)** tells us that if we consider any inner automorphism $\varphi_\tau : S_n \to S_n$, then the cycle types of $\varphi_\tau(\sigma)$ and σ are the same. By considering the contrapositive, we have the desired result.

Problem 13. Observe that in the direct product $G \times H$, every element of the form $((g, e_H))$ commutes with every element of the form (e_G, h). There is a related construction where this is not the case. Let G and H be two groups, and suppose that $\phi : H \to \mathrm{Aut}(G)$ is a homomorphism. We define the semidirect product of G and H (with respect to ϕ) to be the group whose underlying set consists of all elements of the form (g, h), where $g \in G$ and $h \in H$, and whose multiplication is defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot \phi(h_1)(g_2), h_1 h_2).$$

We call this group $G \rtimes_\phi H$, or, when ϕ is understood, $G \rtimes H$

(a) Show that $G \rtimes_\phi H$ is a group
(b) Show that if ϕ is the trivial homomorphism, then $G \rtimes_\phi H = G \times H$
(c) Show that if ϕ is not the trivial homomorphism, then there are elements of the form (e_G, h) and (g, e_H) that do not commute with one another.

Solution 13.

(a) If we consider two arbitrary elements (g_1, h_1) and (g_2, h_2), then $g_1\phi(h_1)(g_2) \in G$ and $h_1 h_2 \in H$. Hence, $(g_1\phi(h_1)(g_2), h_1 h_2)$ belongs to the underlying set $G \times H$, and we may conclude $G \rtimes H$ is closed. The identity element is (e_G, e_H) since $\phi(e_H)$ is always the identity automorphism and $\phi(h)(e_G) = e_G$. The inverse of an element (g_1, h_1) must be (x, h_1^{-1}) where $\phi(h_1)(x) = g_1^{-1}$. Note that we know such x exists because $\phi(h_1)$ is an automorphism. Associativity holds because

$$\begin{aligned}
&= \Big((g_1, h_1)(g_2, h_2)\Big)(g_3, h_3) \\
&= (g_1\phi(h_1)(g_2)\phi(h_1 h_2)(g_3), h_1 h_2 h_3) \\
&= (g_1\phi(h_1)(g_2)\phi(h_1)(\phi(h_2)(g_3)), h_1 h_2 h_3) \\
&= (g_1\phi(h_1)(g_2\phi(h_2)(g_3)), h_1 h_2 h_3) \\
&= (g_1, h_1)\Big((g_2, h_2)(g_3, h_3)\Big)
\end{aligned}$$

(b) Given that ϕ is the trivial homomorphism, then ϕ must map all $h \in H$ to the identity automorphism — an automorphism $f : G \to G$ defined such that $f(g) = g$. Now, consider two arbitrary elements (a, b) and (c, d) in $G \rtimes H$. Then $(a, b)(c, d) = (a\phi(b)(c), bd) = (ac, bd)$, implying both the operation and underdlying set of $G \rtimes H$ is the same as those of $G \times H$. Alternatively, we could say the mapping that maps elements of $G \times H$ to themselves in $G \rtimes H$ is a homomorphism.
(c) Consider the elements $(e_G, h)(g, e_H)$ and $(g, e_H)(e_G, h)$.

$$(g, e_H)(e_G, h) = (g\phi(e_H)(e_G), e_H h) = (g, h) \tag{9}$$

$$(e_G, h)(g, e_H) = (e_G\phi(h)(g), h e_H) = (\phi(h)(g), h) \tag{10}$$

In equation 2, since ϕ isn't the trivial homomorphism, there exists h and g such that $\phi(h)(g) \neq g$. Suppose we chose such h and g. Then, $(g, e_H)(e_G, h) \neq (e_G, h)(g, e_H)$.

Problem 14. Show that there is a homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ with $\phi(1 + 2\mathbb{Z})(k + n\mathbb{Z}) \equiv -k \pmod{n}$. Show that, for this ϕ, we have $(\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (Z/2Z) \cong D_n$.

Solution 14. Consider the homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ defined such that $\phi(0) = e$ and $\phi(1) = g$, where g is the automorphism that maps elements to their inverse ($g(k) \equiv -k \pmod{n}$). To verify that ϕ is, in fact, a homomorphism, consider the four pairs of elements in $\mathbb{Z}/2\mathbb{Z}$. When $a = 0$ or 1 and $b = 1$ or 0 respectively, $\phi(ab) = \phi(a)\phi(b) = g$, and, when $a = 0$ and $b = 0$, $\phi(ab) = \phi(a)\phi(b) = e$. Finally, when $a = 1$ and $b = 1$, $\phi(ab) = e = g^2 = \phi(a)\phi(b)$

To prove that $\mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong D_n$, we consider the map $f : \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \to D_n$ defined such that $f((m,n)) = \rho^m\tau^n$.

$$f\big((a,b)(c,d)\big) = f\big((a\phi(b)(c), bd)\big) = \rho^{a+\phi(b)(c)}\tau^{b+d}$$
$$f\big((a,b)\big)f\big((c,d)\big) = \rho^a\tau^b\rho^c\tau^d$$

Since we're trying to check whether $f\big((a,b)\big)f\big((c,d)\big) = f\big((a,b)(c,d)\big)$, by cancelling ρ^a and τ^d, we need only check that $\tau^b\rho^c = \rho^{\phi(b)(c)}\tau^b$. Suppose $b = 0$. Then, $\tau^b\rho^c = \tau^0\rho^c = \rho^c$ and $\rho^{\phi(0)(c)}\tau^0 = \rho^c$. Suppose $b = 1$. Then $\rho^{\phi(1)(c)}\tau^1 = \rho^{-c}\tau = \tau\rho^c$

$f((m,n)) = e \implies (m,n) = (0,0)$, and, thus, $\ker(f) = \{e\}$. Further, since $|\mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}| = 2n = |D_n|$, we may conclude f is bijective.

Problem 15. Call a 2-cycle in S_n a transposition. We know that transpositions generate S_n, so that every element can be written as a product of transpositions. However, this representation is very far from being unique, and there is no standard way of writing an element as a product of transpositions. Nonetheless, there is one very important invariant to be found in the number of transpositions needed to form a permutation σ. Show that if σ can be written as a product of an even number of transpositions, then every representation of σ as a product of transpositions contains an even number of transpositions. Similarly, if σ can be written as a product of an odd number of transpositions, then every representation of σ as a product of transpositions contains an odd number of transpositions. Show that the permutations that can be written as an even number of transpositions form a subgroup of S_n, called the *alternating group* and denoted A_n.

Solution 15. We know that the identity element can't be written in terms of exactly one transposition, but we do know that it can be written in terms of two. For example, $(ab)(ab) = e$.

Suppose we can write e of the form,

$$e = \alpha_1\alpha_2\alpha_3\ldots\alpha_n$$

where α_m is a transposition.

Now, look at only the elements $\alpha_1 = (a,b)$ and α_2. We can divide the possible values of α_2 into four possible cases: $\alpha_2 = (a,b)$ or (a,c) or (d,b) or (c,d) where $c,d \notin \{a,b\}$

$$(a,b)(a,b) = e$$
$$(a,b)(a,c) = (b,a,c) = (c,b,a) = (c,b)(b,a)$$
$$(a,b)(d,b) = (a,b,d) = (b,d)(d,a)$$
$$(a,b)(c,d) = (c,d)(b,a)$$

In the case where $\alpha_2 = (a,b)$, then we know e can be written in terms of $n-2$ transpositions since $\alpha_1\alpha_2 = e$. For all other cases, we know that we can re-write the transpositions in a form where a is shifted to the right. Let's say upon doing this, $e = \beta_1\beta_2\alpha_3\ldots\alpha_n$. Then, we may simply repeat the process and consider the pair of transpositions β_2 and α_3. If their product is the identity, then we again know that we can write e in terms of $n-2$ transpositions. If not, then we can consider the next pair of elements

Now, suppose keep end up shifting a to the right such that it is on the very end of e. I.e. $e = \beta_1\beta_2\beta_3\ldots(x,a)$. This contradicts the fact that e is the identity since $e(a) \neq x$. Hence, given e can be written in terms of n transpositions, then we know it can be written in terms of $n-2$ transpositions. Further, since e can't be written in terms of one transposition, we know n must be even.

Now consider an arbitrary permutation γ, written in two different forms using transpositions:

$$\gamma = a_1 a_2 a_3 \dots a_n$$
$$\gamma = b_1 b_2 b_3 \dots b_m$$

Since $\gamma\gamma^{-1} = a_1 a_2 a_3 \dots a_n b_m \dots b_3 b_2 b_1 = e$, we know that e can be written in terms $n+m$ transpositions, and, because $n+m$ must be even, we know n and m must both be odd or even.

Now, consider the subset A_n of even permutations in S_n.

- Since the product of two even permutations is simply the product of the transpositions that make up each permutation (in the correct order, of course), then we know that the product of two even permutations is another even permutation.
- The inverse of an even permutation is another permutation with the same transpositions but written backwards (The last transpositions is in the front and the first is in the back). Thus, this inverse must also be an even permutation that may be written through the same number of transpositions.

Thus, A_n must be a group.

Problem 16. Show that the group of symmetries of a tetrahedron is isomorphic to S_4. Show that the group of rotational symmetries of a tetrahedron is isomorphic to A_4.

Solution 16. Consider a tetrahedron and number its four vertices. Every symmetry of the tetrahedron may be defined as a permutation of those vertices, and, hence, all symmetries correspond to elements of S_4. Specifically, for all x in the group of symmetries of a tetrahedron, we define a map f to S_4 such that $f(x)$ is the permutation of vertices produced by the action of x on the vertices of the tetrahedron. It's easy to see why f is a homomorphism, and f is injective because if we have two symmetries that send each vertex to the same place, then they must be equal because symmetries are defined by where they send 3 points. Upon noting that there are $4! = |S_4|$ symmetries of a tetrahedron, we may conclude f is an isomorphism.

We know that all rotations of a tetrahedron can be seen as fixing one of the vertices and rotating the opposing face. Thus, f must send all rotations (barring the identity) to 3-cycles (elements of A_4), and, similarly, all 3-cycles are mapped to rotations under f^{-1} (barring the identity). The required result then follows.

Problem 17. Show that the group of rotational symmetries of a cube is isomorphic to S_4 (What 4 objects get permuted?). Show that the group of all symmetries of a cube is isomorphic to $S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Solution 17. Consider a cube and number its four long diagonals. By permuting these diagonals, we may construct a map f to S_4. f is clearly an isomorphism through the same (or almost the same) argument of **Problem 19**. Further, since we may obtain all symmetries of the cube by considering the rotational symmetries along with a single reflector (any reflection about a plane of symmetry of the cube) multiplied with the rotation symmetries, we may conclude that the group of all symmetries of a cube is isomorphic to $S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Problem 18. For each cycle type in S_6, how many elements of S_6 have the same cycle type?

Solution 18.

Cycle Types	**Number of Elements in Conjugacy Classes of S_6**
$(0,0,0,0,0,1)$	$\frac{6!}{6} = 5! = 120$
$(1,0,0,0,1,0)$	$\frac{6!}{5} = 144$
$(0,1,0,1,0,0)$	$\frac{1}{4} \times (6 \times 5 \times 4 \times 3) = 90$
$(2,0,0,1,0,0)$	$\frac{1}{4} \times (6 \times 5 \times 4 \times 3) = 90$
$(0,0,2,0,0,0)$	$\frac{1}{18} \times (6 \times 5 \times 4) \times 3! = 40$
$(1,1,1,0,0,0)$	$\frac{1}{6} \times (6 \times 5 \times 4) \times 3! = 120$
$(3,0,1,0,0,0)$	$\frac{1}{3} \times (6 \times 5 \times 4) = 40$
$(0,3,0,0,0,0)$	$\frac{1}{24} \times (6 \times 5 \times 4) \times (4 \times 3) = 15$
$(2,2,0,0,0,0)$	$\frac{1}{8} \times (6 \times 5) \times (4 \times 3) = 45$
$(4,1,0,0,0,0)$	$\frac{1}{2} \times (6 \times 5) = 15$
$(6,0,0,0,0,0)$	1

CHAPTER 1.3

Quotient Groups

Exercise 1. Prove Euler's Theorem: if a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Solution. Consider the group $(\mathbb{Z}/n\mathbb{Z})^\times$. We know that the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$, and, by Lagrange's Theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$

Exercise 2. The condition for normality is sometimes written as $g^{-1}Hg = H$, or as $gH = Hg$. Show that these are equivalent to our first definition of normality: A subgroup H of a group G is said to be normal if, for any $g \in G$ and $h \in H$, $g^{-1}hg \in H$.

Solution. Let H be a normal subgroup according to the first definition. Then, consider an element $h \in H$ and an arbitrary $g \in G$. Since $g^{-1}(ghg^{-1})g = h$ and $ghg^{-1} \in H$, $H \subset g^{-1}Hg$. Upon noting $g^{-1}Hg \subset H$ (from our first definition of normality), we have that $g^{-1}Hg = H$ or $Hg = gH$. Now, suppose, for our normal subgroup H, $H = g^{-1}Hg$ by definition. Then it follows that $g^{-1}hg \in H$.

Exercise 3. Let $H < D_3$ be the subgroup of rotations. Then, consider the map $\phi : D_3/H \to \mathbb{Z}/2\mathbb{Z}$, where $\phi(H) = 0$ and $\phi(\tau H) = 1$. Show that ϕ is an isomorphism.

Solution. The proof required for this exercise can be easily generalized to a slightly stronger statement, and, so, we present the generalization instead. All groups of order 2 are isomorphic to $\mathbb{Z}/2\mathbb{Z}$! Let $G = \{e, a\}$ be a group such that $|G| = 2$. Then, consider the map $\phi : G \to \mathbb{Z}/2\mathbb{Z}$, defined such that $\phi(e) = 0$ and $\phi(a) = 1$. We need only show ϕ is a homomorphism since it's apparent that it's a bijective. We do so by considering the four pairs of elements of G.

$$\begin{aligned}
&\phi(aa) = \phi(e) = 0 = 1 \cdot 1 = \phi(a)\phi(a) \\
&\phi(ae) = \phi(ea) = \phi(a) = 1 = 0 \cdot 1 = 1 \cdot 0 = \phi(a)\phi(e) = \phi(e)\phi(a) \\
&\phi(ee) = \phi(e) = 0 = 0 \cdot 0 = \phi(e)\phi(e)
\end{aligned}$$

Since $|D_3/H| = \frac{6}{3} = 2 = |\mathbb{Z}/2\mathbb{Z}|$, the required result follows.

Problem 1. Show that, for $n \geq 2$, $|A_n| = 2$.

Solution 1. Let the set of all odd permutations in S_n be Odd_n. Now, consider the mapping $f : A_n \to \text{Odd}_n$ where $f(a) = \alpha a$ for a fixed $\alpha \in \text{Odd}_n$. We can show that f is injective because $f(a) = f(b) \implies \alpha a = \alpha b \implies a = b$, and, we can see that it's surjective because, for any arbitrary $\beta \in \text{Odd}_n$, $f(\alpha^{-1}\beta) = \beta$. Thus, the cardinality of both sets are equal, and, since A_n and Odd_n are mutually exclusive an exhaustive, we know $2|A_n| = n! \implies |A_n| = \frac{n!}{2}$.

Problem 2. Describe the groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Q}$ as well as you can.

Solution 2. The elements of $\mathbb{Q}/\mathbb{Z}$ contain only elements of the form $x+\mathbb{Z}$ where $0 \leq x < 1$ and $x \in (\mathbb{Q} - (\mathbb{Z}-\{0\}))$. Since $\mathbb{Z}$ is normal, we know that addition of cosets is defined and closed: $x+\mathbb{Z}+y+\mathbb{Z} = (x+y)+\mathbb{Z}$

For $\mathbb{R}/\mathbb{Q}$, similarly, the elements can be represented in the form $x+\mathbb{Q}$ where $0 < x < 1$ and $x \in (\mathbb{R} - \mathbb{Q})$. Closure holds just as it does above, and both quotient groups are of an infinite order.

Problem 3. Suppose that $H, K \trianglelefteq G$, and that $H \cap K = \{e\}$. Show that if $h \in H$ and $k \in K$, then h and k commute.

Solution 3. $h^{-1}khk^{-1} \in H \cap K$. Thus, $h^{-1}khk^{-1} = e \implies kh = hk$

Problem 4. Let G act on a set X, and let $x \in X$. Show that there is a bijection between the cosets of the stabilizer G_x of x and the elements of $\mathrm{O}(x)$, the orbit of x (Prove the Orbit—Stabilizer Theorem).

Solution 4. Consider the map $f : G/G_x \to \mathcal{O}(x)$ such that $f(gG_x) = gx$. Now, suppose $gG_x = g'G_x$. Then, $G_x = g^{-1}g'G_x \implies g^{-1}g' \in G_x$. Thus, $g^{-1}g'x = x \implies g'x = gx$. I.e. f is well defined. f is surjective because for any $y \in \mathcal{O}(x)$, there exists g such that $gx = y$, and, thus, $f(gG_x) = gx = y$. f is injective because $f(g_1G_x) = f(g_2G_x) \implies g_1x = g_2x \implies x = g_1^{-1}g_2x$. Hence, $g_1^{-1}g_2 \in G_x$ and $g_1G_x = g_2G_x$. For finite groups, we may then conclude that $\frac{G}{G_x} = \mathrm{O}(x)$.

Problem 5. Write down all the normal subgroups of D_4 and D_5. For the normal subgroups, identify the quotient as being isomorphic to a more familiar group.

Solution 5. All normal subgroups must be the union of conjugacy classes (where the identity is always included). Thus, an effective way to narrow down the normal subgroups of any group is to list all conjugacy class and test whether the unions of the different combinations of them satisfy the group axioms.

Conjugacy classes of D_4: $\{e\}$, $\{\rho, \rho^3\}$, $\{\rho^2\}$, $\{\tau, \tau\rho^2\}$, $\{\tau\rho^3, \tau\rho\}$

Normal subgroups of D_4: $\{e\}$, $\{e, \rho^2\}$, $\{e, \rho, \rho^2, \rho^3\}$,$\{e, \tau, \rho^2, \tau\rho^2\}$, $\{e, \rho^2, \tau\rho^3, \tau\rho\}$, D_4

Conjugacy classes of D_5: $\{e\}$, $\{\rho, \rho^4\}$, $\{\rho^2, \rho^3\}$, $\{\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$

Normal subgroups of D_5: $\{e\}$, $\{e, \rho, \rho^2, \rho^3, \rho^4\}$, D_5

Quotient Group	**Group Isomorphic to it**
$D_4/\{e\}$	D_4
$D_4/\{e, \rho^2\}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$D_4/\{e, \rho, \rho^2, \rho^3\}$	$\mathbb{Z}/2\mathbb{Z}$
$D_4/\{e, \tau, \rho^2, \tau\rho^2\}$	$\mathbb{Z}/2\mathbb{Z}$
$D_4/\{e, \rho^2, \tau\rho^3, \tau\rho\}$	$\mathbb{Z}/2\mathbb{Z}$
D_4/D_4	Trivial Group

TABLE 1. Groups Isomorphic to the quotient groups of D_4

Problem 6. Suppose $K \trianglelefteq H$ and $H \trianglelefteq G$. Then K is a subgroup of G. Is it necessarily normal? Prove or give a counterexample.

Quotient Group	Group Isomorphic to it
$D_5/\{e\}$	D_5
$D_5/\{e, \rho, \rho^2, \rho^3, \rho^4\}$	$\mathbb{Z}/2\mathbb{Z}$
D_5/D_5	Trivial Group

TABLE 2. Groups Isomorphic to the quotient groups of D_5

Solution 6. Let $G = D_4$, $H = \{e, \tau, \rho^2, \tau\rho^2\}$, and $K = \{e, \tau\rho^2\}$. Then, $H \trianglelefteq G$ and $K \trianglelefteq H$, but K is not normal in G because $\tau\rho\tau\rho^2(\tau\rho)^{-1} = \tau\rho\tau\rho^2\rho^3\tau = \tau\rho\tau\rho\tau = \tau \notin H$

Problem 7. The commutator subgroup $[G, G]$ of G is the subgroup generated by all elements of the form $[g, h] := ghg^{-1}h^{-1}$. (So, it contains all products of elements of the form $[g, h]$). Show that $[G, G] \trianglelefteq G$, and that $G/[G, G]$ is abelian.

Solution 7. Consider an arbitrary element $g \in [G, G]$. For all, $\tau \in G$, $\tau^{-1}g\tau = g\big(g^{-1}\tau^{-1}g\tau\big) = g[g^{-1}, \tau^{-1}] \in [G, G]$. Thus, $[G, G]$ is normal. Now, consider the element $gh[G, G] \in G/[G, G]$. $\forall x \in [G, G]$, $ghx = hg(g^{-1}h^{-1}ghx) \implies gh[G, G] \subset hg[G, G]$. The same argument can be made to show that $hg[G, G] \subset gh[G, G]$. Hence, $hg[G, G] = gh[G, G]$, implying $G/[G, G]$ is normal.

Problem 8. Let G be a finite group. Suppose that $C_1, \ldots, C_r$ are the distinct conjugacy classes of G. Show that $|G| = \sum_{i=1}^{r} |C_i|$. If $C_1, \ldots, C_k$ are the conjugacy classes of size 1, show that $Z(G) = \bigcup_{i=1}^{k} C_i$, and hence that

$$|G| = |Z(G)| + \sum_{j=k+1}^{r} |C_j| .$$

Solution 8. Since conjugacy is an equivalence relation, the conjugacy classes (which are equivalence classes) partiton G. It then holds that $|G| = \sum_{i=1}^{r} |C_i|$. Let $x \in Z(G)$. Then, $g^{-1}xg = xg^{-1}g = x \implies Z(G) \subset \bigcup_{i=1}^{k} C_i$. Let $y \in \bigcup_{i=1}^{k} C_i$. Then, for all $g \in G$, $g^{-1}yg = y \implies yg = gy \implies \bigcup_{i=1}^{k} C_i \subset Z(G)$. Thus, $\bigcup_{i=1}^{k} C_i = Z(G)$ and

$$\left|\bigcup_{i=1}^{r} C_i\right| = \left|\bigcup_{i=1}^{k} C_i\right| + \left|\bigcup_{i=k+1}^{r} C_i\right| = |Z(G)| + \left|\bigcup_{i=k+1}^{r} C_i\right| = |G|.$$

Problem 9. Show that if $|G|$ is a prime power (i.e. p^n for some prime p and integer n), then $Z(G)$ is nontrivial (i.e. $—Z(G)| > 1$).

Solution 9. Consider a group G with an order of p^n. We know that

$$|Z(G)| + \left|\bigcup_{i=k+1}^{r} C_i\right| = |G|$$

When considering the action of G on itself by conjugation, the orbits of G are the conjugacy classes. Thus, the order of all conjugacy classes must divide $|G|$ (Orbit-Stabilizer Theorem), and the order of any non-singleton conjugacy classes are powers of p. Then, because p divides $\left|\bigcup_{i=k+1}^{r} C_i\right|$ and $|G|$, p divides $|Z(G)|$. Hence, $Z(G) > 1$.

Problem 10. Suppose that G is a group and $H \trianglelefteq G$. Show that there is a bijection between subgroups of G/H and subgroups of G that contain H.

Solution 10. Consider a subgroup N of G/H. The union of the cosets of N is a subgroup of G containing H. Let the union of cosets be K. Then, consider $g_1h_1, g_2h_2 \in K$. $g_1h_1g_2h_2 = g_1g_2h_1'h_2 \in K$ (Closure). Further, $(g_1h_1)^{-1} = h^{-1}g^{-1} = g^{-1}h'' \in K$ (Inverses). Lastly, since $H \in N$, $H \subset K$. We now consider the function f from the subgroups of G/H to G, defined such that, for every subgroup N (of G/H), $f(N) = \bigcup_{i \in N} i$. The inverse map would simply be $f^{-1}(A) = A/H$ (where $H \leq A \leq G$). Since f^{-1} exists, we may conclude f is bijective. Further, note that order of $f(N) = |N||H|$.

Problem 11. Show that if $|G| = p^n$ for some prime p, and $k \geq n$,then G has a subgroup H with $|H| = p^k$.

Solution 11. Consider the arbitrary non abelian p-group G where $|G| = p^n$ and its center $Z(G)$. From **Problem 10.**, we know that $Z(G)$ is non trivial, and, hence, it has an order of p^k where $1 \leq k < n$. For all p-groups there exists a subgroup with an order of $p^0 = 1$: the one consisting of only the identity element. Now, assume (inductive hypothesis) that for any p-group with an order less than p^{n-1}, there exists a subgroup of order p^m for all $m \leq n-1$.
By the inductive hypothesis, we've already covered all subgroups of G up to orders of p^k since all subgroups of $Z(G)$ must be subgroups of G. Consider the group $G/Z(G)$ with an order of p^{n-k}. Once again, since $p^{n-k} < p^n$, we know that $G/Z(G)$ has a subgroup for all $n-k+1$ divisors of p^{n-k} by the inductive hypothesis. Further, we can use the bijection f (from **Problem 11.**), from the subgroups of $G/Z(G)$ to the subgroups of G containing $Z(G)$, to show that $\forall K \leq G/Z(G)$, $|f(K)| = |K||Z(G)| = p^\alpha p^k = p^{\alpha+k}$ where $0 \leq \alpha \leq n-k$. Thus, there must exists subgroups in G of the orders $p^k, p^{k+1}, \ldots, p^n$.
This results also holds for abelian p-groups, and the proof would be the exact same but using a non-trivial, proper subgroup H instead of $Z(G)$.

Problem 12. Show that if $G/Z(G)$ is a cyclic group, then G is abelian.

Solution 12. Since $G/Z(G) = \langle xZ(G)\rangle$, $gZ(G) = x^mZ(G) \implies x^{-m}g \in Z(G) \implies \exists z \in Z(G)$, $z = x^{-m}g \implies x^mz = g$.

Now consider two arbitrary elements $h = x^az_1$ and $k = x^bz_2$ in G (where $z_1, z_2 \in Z(G)$)

$$\begin{aligned} hk &= x^az_1x^bz_2 \\ &= x^{a+b}z_1z_2 \\ &= x^bx^az_2z_1 \\ &= x^bz_2x^az_1 \\ &= kh \end{aligned}$$

Hence, G must be abelian.

Problem 13. Show that if p is a prime, then any group of order p^2 is abelian.

Solution 13. Let G be a group such that $|G| = p^2$. Then, $|Z(G)| \in \{p, p^2\}$ (**Problem 10.**). If $|Z(G)| = p^2$, $G = |Z(G)|$. I.e. G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$ and, hence, $|G/Z(G)|$ is cyclic, which implies G is abelian.

Problem 14. Show that $G/Z(G) \cong \text{Inn}(G)$.

Solution 14. We can construct a homomorphism $f : G \to \text{Aut}(G)$ where $\forall g \in G,\ f(g) = \varphi_g$.

For any $g \in Z(G)$, $\varphi_g(h) = ghg^{-1} = h \implies \varphi_g = e$. Thus, $\ker(f) = Z(G)$, and, from the definition of f, $\text{Inn}(G) = \text{im}(G)$.

Hence, by the First Isomorphism Theorem, $G/Z(G) \cong \text{Inn}(G)$.

Problem 15. Lagrange's Theorem states that if $H \leq G$ and G is a finite group, then the order of H divides the order of G. However, the converse is false: if n divides $|G|$, there is not necessarily a subgroup of G of order n. Show that A_4 (which has 12 elements) does not have a subgroup of order 6.

Solution 15.

Conjugacy Classes of A_4 (barring the identity)
$(1,2,3), (1,3,4), (1,4,2), (2,4,3)$
$(1,2,4), (1,3,2), (1,4,3), (2,3,4)$
$(12)(34), (13)(24), (14)(32)$

A subgroup of A_4 with order 6 would have to be normal (because its index is 2), which implies it must be the union of some conjugacy classes. But no such conjugacy classes exist as one might notice from the above table (There aren't any conjugacy classes whose orders sum to 5).

Problem 16. Let a finite group G act on a finite set X. Write X/G for the set of orbits in X, and X^g for the set of elements of X fixed by $g \in G$, i.e. $X^g = \{x \in X : g \cdot x = x\}$. Show that

$$|G| \times |X/G| = \sum_{g \in G} |X^g|.$$

This result is sometimes called Burnside's Lemma, even though it is due to Cauchy. It is also sometimes called "the Lemma that is not Burnside's."

Solution 16.

$$\begin{aligned}
\sum_{g \in G} |X^g| &= \sum_{g \in G} |\{x \in X :\ gx = x\}| \\
&= |\{(x, g) \in X \times G :\ gx = x\}| \\
&= \sum_{x \in X} |g \in G :\ gx = x| \\
&= \sum_{x \in X} |G_x| \\
&= |G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|} \\
&= |G| \sum_{k \in |X/G|} 1 \\
&= |G| \times |X/G|
\end{aligned}$$

Problem 17. Use Burnside's Lemma to count the number of ways to color the edges of a hexagon each either red or blue, where two colorings are considered the same if one is a rotation of the other.

Solution 17. Consider the subgroup of D_6 consisting of only rotations: $H = \{e, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$. To find the total number of distinct colour combinations where two hexagons are the same if one can be rotated onto the other, we simply need to find the total number of orbits in set X - the set consisting of all 2^6 coloured hexagons - when acted upon by H.

$$\sum_{h\in H} \left|X^h\right| = \left|X^\rho\right| + \left|X^{\rho^2}\right| + \left|X^{\rho^3}\right| + \left|X^{\rho^4}\right| + \left|X^{\rho^5}\right| + \left|X^e\right|$$

Begin by numbering the vertices of a regular hexagon clockwise. To find $\left|X^\rho\right|$, our goal should be to find the number of hexagons in X that are unchanged by ρ. We know that these hexagons must have consecutive sides of the same colour, and, thus, there can only be two hexagons invariant under this rotation. Similarly, for ρ^2, the permutation of the sides is $(135)(246)$, implying sides $1, 3,$ and 5 are of the same colour and sides $2, 4,$ and 6 are of the same colour. Hence, there are $2 \times 2 = 4$ number of invariant hexagons under this rotations

Using the same argument for each case, we have

$$\sum_{h\in H} \left|X^h\right| = 2 + 4 + 8 + 4 + 2 + 2^6 = 84$$

and, by Burnside's Lemma,

$$\frac{84}{6} = 14 = |X/H|.$$

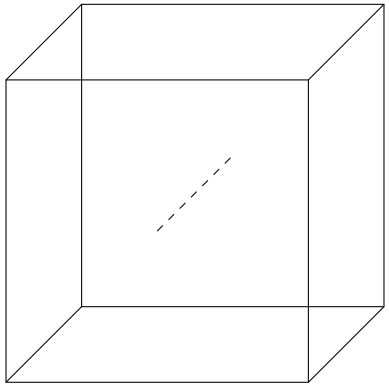
Problem 18. Use Burnside's Lemma to show that there are

$$\frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2)$$

ways of coloring the faces of a cube with n colors (not all the colors have to be used), if two colorings are considered equivalent if you can rotate one to get the other.

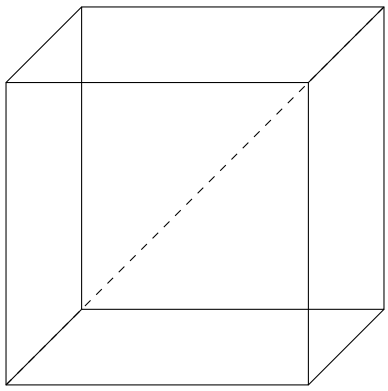
Solution 18. We can make a similar argument to that of **Problem 19.** by considering the various types of rotations of a cube. Specifically, we can make three major groups of rotations:

(1) Rotations about an axis passing through the centres of opposite faces
(2) Rotations about an axis passing through two vertices
(3) Rotations about an axis passing through the mid-points of edges.



Consider the above cube and one its axes (the dashed line). There are three possible rotations about this axis; two of which take a face to its adjacent face and one of which take a face to its opposite face (all three

fix the faces the axis passes through). Thus, there are $2n^3 + n^4$ possible cubes that are unchanged by the rotations about this axis. Further, there $3(2n^3 + n^4)$ possible cubes unchanged by all rotations of category 1 since only three distinct axes pass through the centres of opposite faces.



Once again, consider the above cube and the axis shown. A rotation about this axis fixes no face and always sends one face to an adjacent face that it shares a vertex with (this vertex is always one of the two vertices the axis passes through). Hence, there are two possible rotations that leave $2n^2$ cubes fixed. Further, there are 4 possible axes that allow for rotations of category 2, and, hence, $8n^2$ cubes are fixed by the rotations of category 2.

Using, a similar method with axes of category three, we find that $6n^3$ cubes are fixed.

Overall,

$$\sum_{g\in G} |X^g| = 3(2n^3 + n^4) + 8n^2 + 6n^3 + n^6 = n^6 + 3n^4 + 12n^3 + 8n^2$$

where X is the set of all n^6 coloured cubes and G is the group of rotations of the cube.

Hence, by Burnside's Lemma,

$$24 \times \big|X/G\big| = n^6 + 3n^4 + 12n^3 + 8n^2 \implies \big|X/G\big| = \frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2)$$

Problem 19. How many graphs are there on four vertices, up to isomorphism?

Solution 19. For simplicity, it might help to think of every simple graph with four vertices by fixing the vertices to form a square shape. Then, we may draw lines between the various vertices of the square to create any graph. Clearly, it's possible to generate all possible graphs upto isomorphism like this, but, within the set of square graphs, there will be graphes that are isomorphic to each other. In fact, if we consider the action of S_4 on these squares, then the orbits contain squares that are isomorphic to each other. Hence, our goal is to find the total number of orbits.

Since all elements of the same conjugacy class fix the same number of elements, we can simply take an example from each of the five conjugacy classes, find the elements of X that are fixed by this example, and multiply by the number of elements in said conjugacy class. Upon doing so, we find there are

$$\frac{1}{|G|}\sum_{g\in G} |X^g| = \big|X/G\big| = \frac{264}{24} = 11$$

simple graphs up to isomorphism.

Problem 20. Show that the 15 puzzle is not solvable.

Solution 20. Our goal is to show that it is impossible to solve the below puzzle:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	E

For all jumbled start positions with a solution, we know that it's possible to move the tiles from the start position back to the jumbled position, and, further, we know that all valid moves can be represented as a product of transposition involving the empty position. For example, to represent the move switching 15 and E (the empty position), we'll use the transposition $(E, 15)$. The product of multiple of these valid moves results in a permutation, who's action on the Fifteen Puzzle in its solved state creates a solvable jumbled state.Since the empty position has to start and end at the same place, we know that it's journey while moving from the solved position to the jumbled position (or vice verse) must include an up for every down and a left for every right it makes. Thus, for any $\sigma \in S_{16}$ that takes a jumbled position to a solved position, we know that it must be able to be represented as a product of even transpositions containing E. In other words, all jumbled positions that require an odd permutation to take it to the solved position are not solvable. Thus, the puzzle requiring us to switch 14 and 15 is impossible to solve.

CHAPTER 1.4

Group Actions & The Sylow Theorems

Problem 1. Show that there is an injective homomorphism $f : S_m \times S_n \to S_{m+n}$.

Solution 1. Suppose we let the elements of $S_m \times S_n$ act on the two sets of objects $\{1, 2, 3, \ldots, m\}$ and $\{m+1, m+2, \ldots, m+(n-m)\}$. Specifically, the element (σ_1, σ_2) acts by letting σ_1 permute the objects $\{1, 2, 3, \ldots, m\}$ and σ_2 permute the objects $\{m+1, m+2, \ldots, m+(n-m)\}$. This allows us to define a homomorphism $f : S_m \times S_n \to S_{m+n}$. Note that f is injective because the only element that fixes all objects is (e, e).

Problem 2. Suppose that G acts transitively on X. Suppose further that for all $g \in G \backslash \{e\}$ and all $x \in X$, $gx \neq x$. Show that $|G| = |X|$. We call X a G-torsor.

Solution 2. Since the action of G on X is transitive, there exists only one orbit in X. I.e. $|X| = |\mathcal{O}(x)|$. Further, for this same x, we know that $\text{stab}(x) = \{e\}$. By the Orbit-Stabilizer Theorem, we then have that $|\mathcal{O}(x)| = |G| \implies |X| = |G|$.

Problem 3. Prove Proposition 4.3. — $N_G(H) \leq G$ and, in fact, $N_G(H)$ is the largest subgroup K of G such that $H \trianglelefteq K$.

Solution 3.

- $\forall g_1, g_2 \in N_G(H) : \; g_1 g_2 H g_2^{-1} g_1^{-1} = g_1 H g_1^{-1} = H \implies g_1 g_2 \in N_G(H)$
- $\forall g \in N_G(H) : \; eHe = H \implies g^{-1} g H g^{-1} g = H \implies g^{-1} H g = H \implies g^{-1} \in N_G(H)$

Hence, $N_G(H)$ must be a subgroup of G. Further, from its definition, it must be the largest possible group in which H is normal because it includes all g such that $gHg^{-1} = H$.

Problem 4. Find a surjective homomorphism $\phi : S4 \to S3$.

Solution 4. Let S_4 acts on the conjugacy class X (of itself) of permutations with cycle types $(0, 2, 0, 0)$ by conjugation. Then, we may construct a homomorphism from S_4 to $S_{|X|} = S_3$.

Problem 5. Suppose that G acts transitively on X. A block is a nonempty subset B of X so that, for every $g \in G$, either $gB = B$ or $gB \cap B = \phi$.

(a) If B is a block, show that $G_B = \{g \in G : gB = B\}$ is a subgroup of G. Show that if $x \in B$, then $G_x \leq G_B$.

(b) If B is a block, and $B = B_1, B_2, \ldots, B_r$ are the distinct images of B under the action of G, then the B_i's form a partition of X.

(c) We call the action of G on X *primitive* if the only blocks are X itself and subsets of size 1. Is the action of D_4 on the vertices of a square primitive?

Solution 5.

(a) • $\forall g_1, g_2 \in G_B : \; g_1 g_2 B = g_1 B = B$

- $\forall g \in G_B:\ eB = B \implies g^{-1}gB = B \implies g^{-1}B = B$

  Hence, G_B is a subgroup of G. Now, for $x \in B$, consider $g \in G_x$. Since $gx = x$, $gB \cap B = \{x\} \implies gB = B$. Hence, $g \in G_B \implies G_x \leq G_B$.

(b) Since G acts transitively on X, we know that, for any given x, there exists g such that $x \in gB$. Further, $B_i \cap B_k = \phi$. Hence, the images of B must partition X.

(c) Let X be the set of vertices of a square. If we consider the element ρ acting on the subsets of X, then a non trivial block in X must be subset of size 2 — more specifically, it must consist of opposite vertices. Now, we can check that the definition of a block is met with every other element of D_4 to show that our group action isn't primitive.

Problem 6. Is a Sylow 2-subgroup of A_4 isomorphic to a group you recognize? If so, which one? How about a Sylow 2-subgroup of S_4?

Solution 6. Recall Lemma 0.1.2. While this may seem unrelated to the problem, this gives us an easy way to see what the Sylow 2-subgroups of A_4 are isomorphic to. There are no elements with an order of 4 in A_4, and, hence, all possible Sylow 2-subgroups must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In S_4, the Sylow 2-subgroup $\langle (13), (1234) \rangle$ is isomorphic to D_4 since $(1234)(13) = (13)(1234)^3$. Note that constructing a bijective homomorphism from D_4 to $\langle (13), (1234) \rangle$ is now fairly straight forward.

Problem 7. How many Sylow 2-subgroups does S_4 have? How about A_4?

Solution 7. Upon listing the elements of $\langle (13), (1234) \rangle$, we can see that it isn't the union of conjugacy classes and, hence, isn't normal. Thus, $n_2(S_4) = 3$ by Sylow 3. Similarly, we can take an example of a Sylow 2-subgroup in A_4: $\{e, (12)(34), (13)(24), (14)(23)\}$. As you might notice, this subgroup is the union of two conjugacy classes ($\{(12)(34), (13)(24), (14)(23)\}$ and $\{e\}$) and is, hence, normal. Thus, $n_2(A_4) = 1$ by Sylow 3.

Problem 8. If p is an odd prime, show that every Sylow p-subgroup of D_n is cyclic and normal.

Solution 8. Consider an odd prime p dividing $|D_n|$. Let K by a Sylow p-subgroup. Since $2 \nmid |K|$, no elements of order 2 belong in K. Thus, K contains no rotaions and must be a subgroup of the group of rotations. By Lemma 0.1.3, K must then be cyclic. Further, we know K must be normal because the conjugate of any element in K is either itself or its inverse.

Problem 9. If $P \in \mathrm{Syl}_2(D_n)$, show that $N_{D_n}(P) = P$.

Solution 9. From **Problem 11.**, $n_2(D_n) = m$. Suppose $D_n = 2^a m$. Then, for some Sylow 2-subgroup P,

$$n_2(P) = \frac{|D_n|}{|\mathrm{N}_{D_n}(P)|} \implies m = \frac{2^a m}{|\mathrm{N}_{D_n}(P)|} \implies |\mathrm{N}_G(P)| = 2^a.$$

Hence, the relationship $P \trianglelefteq N_{D_n}(P)$ becomes an equality: $P = N_{D_n}(P)$

Problem 10. How many Sylow 2-subgroups does D_n have? (You may wish to classify n by writing $2n = 2^a m$, where m is odd.)

Solution 10. Suppose $|D_n| = 2^a m$ where m is odd. Consider the group of symmetries of an n-gon with an order of $2^a m$ and a k-gon with an order of 2^a ($D_n = D_{2^{a-1}m}$ and $D_{2^{a-1}}$). There are exactly m regular k-gons that can be inscribed within the n-gon such that the vertices of the polygons lie on each other, and there exists a subgroup of $D_{2^{a-1}m}$ that are the symmetries of a given inscribed k-gon. This is one possible Sylow

2-subgroup of D_n. There at least m of these kinds of subgroups for each of the k-gons. Since $n_2(D_n) \leq m$, we have that $n_2(D_n) = m$.

Problem 11. Let p be an odd prime. Describe a Sylow p-subgroup of S_p and S_{2p}. How many are there?

Solution 11. In S_p, the Sylow p-subgroups are of order p. Hence, they must be cyclic and contain only elements of order p (barring the identity). Further, every element of a given Sylow p-subgroup must generate it. Thus,

$$n_p(S_p) = \frac{(p-1)!}{p-1} = (p-2)!$$

This is technically unrelated, but, by using this information, we can rather easily show Wilson's Theorem: $(p-2)! \equiv 1 \mod p \implies (p-1)! \equiv -1 \mod p$.

In S_{2p}, the Sylow p-subgroups must be of order p^2. As an example, consider the group $\langle (1,2,3,\ldots,p), (p+1, p+2, p+3, \ldots, p+p)\rangle$. Since the generators are disjoint cycles, the group must be abelian. Further, all other Sylow p-subgroups must also be abelian and must be represented as a group generated by two permutations of order p. Hence, to find the number of Sylow p-subgroups, we need not do more than answer two simple questions. How many possible groups can we create as a combination of two disjoint permutations of order p? How many of such groups are the same?

By answering those questions, we get

$$n_p(S_{2p}) = \frac{(2p)!}{2(p-1)^2p^2}$$

Problem 12. Investigate a Sylow p-subgroup of S_{p^2}. Show that this group is nonabelian. This group is an example of a wreath product, which I think of as the symmetries of a chandelier: you can permute the lights within each arm of the chandelier, and then you can also permute the arms.

Solution 12. The order of the sylow p-subgroups of S_{p^2} is p^{p+1}. We can construct a group of order p^p by using p disjoint p-cycles as generators. As an example, consider the group

$$H = \langle (1,2,3,\ldots,p), (p+1, p+2, p+3, \ldots, 2p), \ldots, (p(p-1)+1, p(p-1)+2, p(p-1)+3, \ldots, p^2)\rangle.$$

Now, suppose we chose σ in S_{p^2} and considered the subgroup $N = \langle (1,2,3,\ldots,p), (p+1, p+2, p+3, \ldots, 2p), \ldots, (p(p-1)+1, p(p-1)+2, p(p-1)+3, \ldots, p^2), \sigma\rangle$. At most, $|N| = p^{p+1}$, but it may be that for some $x, y \in H$, $x\sigma^i = y\sigma^m$ ($i, m < |\sigma|$ and $i < m$). Since $x\sigma^i = y\sigma^m \iff y^{-1}x = \sigma^{m-i} \iff \sigma \in H$, we must choose $\sigma \notin H$. One such σ is the permutation

$$(1, 2p+1, 3p+1, \ldots, p(p-1)+1)(2, 2p+2, 3p+2, \ldots, p(p-1)+2)\ldots(p, 2p, 3p, \ldots, p^2).$$

Upon noting $((1,2,3,\ldots,p)\sigma)(1) = 2p+1 \neq 2p+2 = (\sigma(1,2,3,\ldots,p))(1)$, we have that N is nonabelian.

Problem 13. Show that if $N \trianglelefteq G$, then $n_p(G/N) \leq n_p(G)$.

Solution 13. Now, consider the mapping f from the subgroups of G/N to the subgroups of G containing N. From the conventional definition of f, it holds that $|f(K)| = |K||N|$. Thus, if we consider a Sylow p-subgroup K of G/N, then $f(K)$ must be a subgroup of G such that the Sylow p-subgroups of $f(K)$ are also Sylow p-subgroups of G.
Now, suppose there exists a Sylow p-subgroups L and M of G/N such that $f(L)$ and $f(M)$ share a Sylow p-subgroup P. Let $|L|, |M| = p^\alpha m$ and $N = p^\beta n$. From Lemma 0.1.4,

$$\frac{|P||N|}{|P \cap N|} = \frac{p^{\alpha+\beta}n}{p^\alpha} = p^\beta n = |PN|,$$

and, since $PN \leq M$, $PN = M$. Similarly, $PN = L$, and, thus, $M = L$. We can then conclude that $n_p(G/N) \leq n_p(G)$.

Problem 14. Show that if $n_p(G) \not\equiv 1 \pmod{p^2}$, then there are distinct Sylow p-subgroups P and Q of G such that $[P : P \cap Q] = [Q : P \cap Q] = p$.

Solution 14. Let the sylow p-subgroup P (where $|P| = p^n$) act on $\mathrm{Syl}_p(G)$ by conjugation. Then, we can write $\mathrm{Syl}_p(G)$ in terms of n distinct orbits: $\mathrm{Syl}_p(G) = O_1 \cup O_2 \cup O_3 \cup \cdots \cup O_n$. Let a representative of the orbit O_i be P_i.

To begin, $|O_i| = |P : \mathrm{N}_P(P_i)|$. Now, consider an element $x \in N_P(P_i)$, and note that $\langle x \rangle P_i$ must be a p-subgroup, implying $\left|\langle x \rangle P_i\right| \leq p^n$. Because $|P_i| = p^n$ and $P_i \leq \langle x \rangle P_i$, we have $\left|\langle x \rangle P_i\right| = p^n \implies \langle x \rangle P_i = P_i \implies x \in P_i$. Further, since $P \cap P_i \subset \mathrm{N}_P(P_i)$ and $\mathrm{N}_P(P_i) \subset P \cap P_i$, we have $P \cap P_i = \mathrm{N}_P(P_i)$ and, thus, $|O_i| = |P : P \cap P_i|$

Now, we can say $|\mathrm{Syl}_p(G)| = |P : P \cap P_1| + |P : P \cap P_2| + |P : P \cap P_3| + \cdots + |P : P \cap P_n|$. Let $P_1 = P$. Then, we have $|\mathrm{Syl}_p(G)| = 1 + p^{\alpha_2} + p^{\alpha_3} + \cdots + p^{\alpha_n}$ where $\alpha_i \neq 0$ (If it did, then that would imply $P_i = P$). If we assume that all $\alpha_i > 1$, then we have $n_p(G) \equiv 1 \mod p^2$. Thus, there must exist some $\alpha_i = 1$, and, hence, some P_i such that $|P : P \cap P_i| = p$

Problem 15. Let k be a positive integer. An action of G on X is said to be k-transitive if for any $x_1, \ldots, x_k$ of distinct elements of X and any $y_1, \ldots, y_k$ of distinct elements of X, there is some $g \in G$ so that $g \cdot x_i = y_i$ for $1 \leq i \leq k$.

(a) Show that the action of S_n on $\{1, \ldots, n\}$ is k-transitive for any $k \leq n$
(b) Show that the action of A_n on $\{1, \ldots, n\}$ is k-transitive for any $k \leq n - 2$.
(c) Can you find any other group actions that are 2-transitive?

Solution 15. Note that an action being k-transitive implies that it's also i-transitive for all $i \leq k$. Hence, for parts (a) and (b), we need only show the mentioned group actions are k- transitive where k is the upper bound.

(a) Elements of S_n are defined by where they send $\{1, \ldots, n\}$. Thus, the action of S_n on $\{1, \ldots, n\}$ must be n-transitive.
(b) There are two elements in S_n that send a specific $x_1, x_2, x_3, \ldots, x_{n-2}$ to a specific $y_1, y_2, y_3, \ldots, y_{n-2}$. Call these two elements σ and τ and call the two elements that aren't in the x's a and b and the two that aren't the y's c and d. If we let $\sigma(a) = c$, $\sigma(b) = d$, $\tau(a) = d$, and $\tau(b) = c$, then $\sigma(cd) = \tau$. Hence, if σ was odd then τ must be even and vice versa. I.e. σ or τ must be in A_n (only one - not both) and the mentioned action is $(n-2)$-transitive.
(c) The group of similarities of $\mathbb{R}^2$ acting on the points of $\mathbb{R}^2$ is 2-transitive.

Problem 16. Show that if G is a nonabelian simple group of order less than 100, then $|G| = 60$. (Hint: classify numbers based on the form of their prime factorizations. The case of $|G| = 90$ is tricky.)

Solution 16. Recall Lemma 0.1.5. It will be of use here. Given that $|G| \leq 100$, it must hold that $|G| \in \{p^n, p^n q^m, pqr, p^2qr, pq^2r\}$ where p,q, and r are primes such that $p < q < r$. We'll break our problem into cases to proceed.

(1) $|G| = p^n$. Since we're only working with non-abelian groups, it suffices to state that the $Z(G)$ must be a non trivial normal subgroup of G, and, hence, G can't be simple.
(2) $|G| = pq^m$. $n_q(G) = 1$ because $1 < p < q$, and G can't be simple.
(3) $|G| = p^2q$. Given $n_q(G) = p^2$ (It can't be p), we have $p^2q - p^2(q-1) = p^2$ number of elements of order p, p^2, or 1. This leaves only only sylow p-subgroup, and, hence, G must be normal.
(4) $|G| = p^2q^2$. Since $|G| \leq 100$, we have $|G| = 36 = 2^2 \times 3^2$ or $100 = 2^2 \times 5^2$. When $|G| = 100$, $n_5(G) = 1$ by sylow 3. Now suppose $|G| = 2^2 \times 3^2$. Assuming $n_3(G) = 4$, we can let G act on

$\text{Syl}_3(G)$ by conjugation and set up a homomorphism $\phi : G \to S_4$. ϕ isn't trivial, and we know that $\ker(\phi) = \frac{|G|}{\text{im}(\phi)}$. Since $|\,\text{im}(\phi)| \neq |G|$ because $|G|$ is too big, $\ker(\phi)$ is a non trivial normal subgroup.

(5) $|G| = p^3q$. Since $|G| \leq 100$, we have $|G| \in \{24, 40, 56, 88\}$. When $G = 88$, $n_{11}(G) = 1$. Similarly, when $|G| = 40$, $n_5(G) = 1$. When $|G| = 56$, $n_7(G) = 8$ and that leaves $56 - 48 = 8$ elements of order 1, 2, 2^2, and 2^3 and only 1 sylow 2-subgroup. When $|G| = 24$, $n_3(G) = 4$ and, hence, we can let G act on $\text{Syl}_3(G)$ by conjugation to setup a homomorphism $\phi : G \to S_4$ where $\ker(\phi)$ is a non trivial normal subgroup.

(6) $|G| = p^3q^2$. Once again, since $|G| \leq 100$, $|G| = 72 = 2^8 \times 3^2$, and, just as before, we must have 4 sylow 3-subgroups. We may, then, let G act on $\text{Syl}_3(G)$ by conjugation and set up a homomorphism $\phi : G \to S_4$ where $\ker(\phi)$ is a non trivial normal subgroup.

(7) $|G| = p^4q$. Assume $|G| = 48 = 2^4 \times 3$ and $n_2(G) = 3$. Once again, let G act on $Syl_2(G)$ by conjugation so that we may define a homomorphism $\phi : G \to S_3$ such that $\ker(\phi)$ is a non trivial normal subgroup.
Assuming $|G| = 86 = 2^4 \times 5$, we have $n_5(G) = 16$, and this leaves only one sylow 2-subgroup.

(8) $|G| = p^5q$. Assume $|G| = 96 = 2^5 \times 3$. Once again, upon assuming $n_2(G) = 3$, we can set up a homomorphism $\phi : G \to S_3$ where $\ker(\phi)$ is a non trivial normal subgroup by letting G act on $\text{Syl}_3(G)$ by conjugation.

(9) $|G| = pqr$. Assume $n_r(G) = pq$ and $n_q(G) = pr$. Then, the number of elements of order q or r must be $pq(r-1) + pr(q-1) = 2pqr - pq - pr$ - which is greater than $pqr = |G|$
Now, assume $n_q(G) = r$ instead. Then, the number of elements of order p is $pqr - \big(pq(r-1) + r(q-1)\big) = q(p-r) + r - 1$ - which is less than r. This forces us to say that $n_p(G) = q$ and that $q(p-1) = q(p-r) + r - 1 \implies p - 1 = p - r + \frac{r-1}{q} \implies 1 = r - \frac{r-1}{q} \implies 1 - r = \frac{1-r}{q} \implies q = 1$, but q must be prime. Overall, there are no simple groups that can be written as the product of three primes.

(10) $|G| = p^2qr$. Here, $|G| \in \{60, 84\}$. If $|G| = 84 = 4 \times 3 \times 7$, then $n_7(G) = 1$ and, hence, G can't be simple. If we assume $|G| = 60$, then it's indeed possible for G to be simple. As an example, consider A_5.

(11) $|G| = pq^2r$. Here, $|G| = 90 = 2 \times 3^2 \times 5$ (This is the only prime factorization, of this form, less than 100). Using sylow 3 alone, we know $n_5(G) = 6$ and $n_3(G) = 10$. If we assume that the intersection of all sylow 3 subgroups is trivial, then we reach an apparent contradiction: there are $10(9-1) + 6(5-1) = 104$ elements in G. Now, suppose there are two distinct sylow 3-subgroups H and K such that $|H \cap K| = 3$. Since $|H : H \cap K|$ is the smallest prime that divides $|H|$, we know that $H \cap K$ must be normal in H (and K using the same argument). We have that $N_G(H \cap K)$ has the following properties:
- $|N_G(H \cap K)| \geq 27$
- $9 \mid |N_G(H \cap K)|$
- $|N_G(H \cap K)| \mid |G|$

Hence, $|N_G(H \cap K)| \in \{45, 90\}$. If $N_G(H) = 45$, then $N_G(H)$ has index 2 and must be normal. If $N_G(H) = 90$, then $N_G(H) = G$ and $G \cap K$ is normal.

CHAPTER 1.5

Abelian Groups

Problem 1. Compute $\gcd(5371, 7598)$. If the gcd is d, find integers a and b such that $5371a + 7598b = d$.

Solution 1. Upon applying the euclidean algorithm, we have that

$$\begin{aligned}\gcd(7598, 5371) &= \gcd(7598, 5371)\\ &= \gcd(2227, 5371)\\ &= \gcd(2227, 3144)\\ &= \gcd(2227, 917)\\ &= \gcd(1310, 917)\\ &= \gcd(393, 917)\\ &= \gcd(393, 524)\\ &= \gcd(393, 131)\\ &= \gcd(262, 131) = \gcd(131, 131) = 131\end{aligned}$$

By keeping track of our steps, we have that $131 = -12 \times 7598 + 17 \times 5371$.

Problem 2. Find a simultaneous solution to the congruences

$$x \equiv 4 \pmod{11}, \quad x \equiv 5 \pmod{12}, \quad x \equiv 9 \pmod{16}.$$

Solution 2. By inspection, $x = -7$.

Problem 3. Prove that the fraction $\frac{21n+4}{14n+3}$ is in lowest terms, for every positive integer n. (IMO 1959)

Solution 3. This is probably one of the easiest IMO Problems. $\frac{21n+4}{14n+3}$ is completely reduced for all n if and only if $\gcd(21n + 4, 14n + 3) = 1$ for all n. Upon applying the euclidean algorithm, we have that

$$\begin{aligned}\gcd(21n + 4, 14n + 3) &= \gcd(7n + 1, 14n + 3)\\ &= \gcd(7n + 1, 7n + 2)\\ &= \gcd(7n + 1, 1) = 1\end{aligned}$$

Problem 4. Show that the classification of finite abelian groups can be restated as follows: if G is a finite abelian group, then there exist numbers $n_1, n_2, \ldots, n_k$ with $n_i \mid n_{i+1}$ for each $1 \leq i < k$, such that

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}).$$

Solution 4. Suppose we have that all finite abelian groups can be written as $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \mathbb{Z}/n_m\mathbb{Z}$ where the n_i's are invariant factors. Then, by writing the n_i's as there prime factorizations, we can break up the $\mathbb{Z}/n_i\mathbb{Z}$ into cyclic groups of prime power order. For example, given that $n_i = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_r^{e_r}$, we have that $\mathbb{Z}/n_i\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$ via the Chinese remainder theorem.

Now, suppose that all finite abelian groups can be written as the product of cyclic groups of prime power order. For a finite abelian G, begin by combining the cyclic groups of the highest prime power order to

create one cyclic group. Do the same for the second highest prime powers for each prime, and so on. Then, we would have written G as $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$ where $n_i | n_{i+1}$.

Problem 5. Show that any finite group has a normal series such that all the quotients are simple.

Solution 5. Suppose we have a composition series and two consecutive groups G_i and G_{i+1}. Assuming that G_{i+1}/G_i is not simple. I.e. we have a non trivial normal subgroup $H \leq G_{i+1}/G_i$. By using the bijection that sends the subgroup of G_{i+1}/G_i to the subgroup of G_{i+1} containing G_i, we know there exists a subgroup K such that $G_i \triangleleft K \leq G_{i+1}$. Now, let's consider the two homomorphisms ϕ and φ. $\phi : G_{i+1} \to G_{i+1}/G_i$ where $\phi(x) = xG_i$. Similarly, $\varphi : G_{i+1}/Gi \to \big(G_{i+1}/G_i\big)/H$ where $\varphi(x) = xH$. Given that $\phi(\varphi(x)) = e$, we have that $x \in K$ and $K = \ker(\varphi\phi)$. Thus, $K \triangleleft G_{i+1}$, and we have a contradiction: our normal series is not a composition series.

Problem 6. Show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution 6. Consider the map $f : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ where $f(\lambda) = \lambda(1)$. We know our map is injective because $\lambda(1) = \alpha(1) \implies \lambda = \alpha$. I.e. by defining where we send 1, we know where all other elements are sent, and, hence, we've defined our automorphism. Further, our map is also surjective because there are exactly $\phi(n)$ possible automorphisms since 1 must be sent to a generator of $\mathbb{Z}/n\mathbb{Z}$.

We also have that f is a homomorphism (and an isomorphism) because

$$\begin{aligned} f(\lambda\alpha) &= \lambda(\alpha(1)) \\ &= \underbrace{\lambda(1) + \lambda(1) + \cdots + \lambda(1)}_{\alpha(1) \text{ times}} \\ &= \lambda(1)\alpha(1) \mod n = f(\lambda(1))f(\alpha(1)) \end{aligned}$$

Problem 7. Find a polynomial with coefficients in $\mathbb{Z}/n\mathbb{Z}$ of degree $d > 0$ with more than d distinct roots in $\mathbb{Z}/n\mathbb{Z}$. In terms of n and d, what is the maximum number of roots? (Or, at least, find a construction that gives you many roots.)

Solution 7. Consider the polynomial x^3 in $\mathbb{Z}/8\mathbb{Z}$. $x^3 = 0 \implies x \in \{0, 2, 4, 6\}$. Now, consider an arbitrary polynomial $f(x)$ in $\mathbb{Z}/n\mathbb{Z}$ where $n = p_1p_2p_3 \dots p_r$ and $p_i = p_k \implies i = k$ (also note that the p_i's are larger than d — the degree of f). To find the roots of f, we may first consider the roots of f in $\mathbb{Z}p_i\mathbb{Z}$ for all i and use the Chinese Remainder theorem to find the find roots in $\mathbb{Z}/n\mathbb{Z}$. The maximum number of roots of f in $\mathbb{Z}/p_i\mathbb{Z}$ is d; so, we have that the maximum number of roots of f in $\mathbb{Z}/n\mathbb{Z}$ is d^r.

Problem 8. Let $a_n = 100 + n$. What is the largest possible value of $\gcd(a_n, a_{n+1})$, where n runs over the positive integers? (AIME 1985)

Solution 8.

$$\begin{aligned} \gcd(a_n, a_{+1}) &= \gcd(a_n, a_{n+1} - a_n) \\ &= \gcd(100 + n^2, 2n + 1) \\ &= \gcd(100 + n^2 - 100(2n + 1), 2n + 1) \\ &= \gcd(n^2 - 200n, 2n + 1) = \gcd(n(n - 200), 2n + 1) \end{aligned}$$

Since n and $2n+1$ are relatively prime,

$$\begin{aligned}\gcd(n(n-200), 2n+1) &= \gcd(n-200, 2n+1)\\ &= \gcd(n-200, 401)\end{aligned}$$

Thus, $\gcd(a_n, a_{n+1})$ is at most 401.

Problem 9. A lattice point $(x, y) \in \mathbb{Z}^2$ is said to be blocked if $\gcd(x, y) > 1$. Show that, for any positive integer n, there is an $n \times n$ square consisting entirely of blocked points (for example, $(14, 20)$, $(14, 21)$, $(15, 20)$, $(15, 21)$ is a 2×2 square of blocked points).

Solution 9. Our goal is to pick (a, b) such that $gcd(a + k, b + j) \neq 1$ for all $k, j \leq n$, and to do so, we need n^2 distinct primes $p_1, p_2, \ldots, p_{n^2}$. We must have that, for all $(a + k, b + j)$, $a \equiv -k \mod p_i$ and $b \equiv -j \mod p_i$. This leaves us with n^2 congruences on a and b, and, by the Chinese Remainder theorem, we know they can be solved. (Note that we may have that certain congruences imply others.)

Problem 10. A positive integer n is said to be abundant if the sum of the divisors of n is greater than $2n$. Show that, for any positive integer k, it is possible to find k consecutive abundant numbers.

Solution 10. Let the prime factorization of n be $p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_m^{e_m}$, and let $\sigma(n)$ be the sum of the divisors of n.

We have that

$$\sigma(n) = \prod_{k=1}^{m} \sum_{i=0}^{e_k} p_k^i = \frac{1 - p_1^{e_1+1}}{1 - p_1} \times \frac{1 - p_2^{e_2+1}}{1 - p_2} \times \cdots \times \frac{1 - p_m^{e_m+1}}{1 - p_m} = \prod_{i=1}^{k} \sigma(p_i^{e_i})$$

Now, for n to be abundant, we must have that $\frac{\sigma(n)}{n} > 2$. We have that $\frac{\sigma(kn)}{kn} = \frac{\sigma(k)\sigma(n)}{kn}$ (given k and n are relatively prime). Hence, (since $\frac{\sigma(n)}{n}$ can't be less than 1) we have that certain multiples of abundant numbers are abundant.

Alternatively, we can see that if n is abundant, then $\sigma(n) \geq 2n \implies k\sigma(n) \geq 2kn$. And, since $\sigma(kn) \geq k\sigma(n)$, we have that kn is abundant for all k.

Now, all we need is k $(q_0, q_1, \ldots, q_{k-1})$ relatively prime abundant numbers because, by the Chinese Remainder theorem, we know there must exist an N such that

$$\begin{aligned}N &\equiv 0 \mod q_0\\ N &\equiv -1 \mod q_1\\ &\vdots\\ N &\equiv -k \mod q_{k-1}\end{aligned}$$

Now, let p_i be the ith prime.

$$\begin{aligned}\prod_i \frac{\sigma(p_i)}{p_i} &= \prod_i \frac{1-p_i^2}{1-p_i} \times \frac{1}{p_i} \\ &= \prod_i \frac{1+p_i}{p_i} \\ &= \prod_i \frac{1}{p_i} + 1 \\ &\geq \sum_i \frac{1}{p_i}\end{aligned}$$

Hence, he infinite product $\prod_i^\infty \frac{\sigma(p_i)}{p_i}$ diverges to positive infinity, and it's possible to pick k relatively prime abundant numbers. The requried result then follows.

Problem 11. Prove that for each positive integer n, there are pairwise relatively prime positive integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \ldots k_n - 1$ is the product of two consecutive integers. (USAMO 2008)

Solution 11. Begin by inducting on n. For the base case ($n = 1$), simply consider the integer $k_1 = m^2 + m + 1$ for any integral m. Now, we assume that $k_1 k_2 \ldots k_n = m^2 + m + 1$ and let $k_{n+1} = (m+1)^2 + (m+1) + 1 = m^2 + 3m + 3$.

Firstly,

$$\begin{aligned}\gcd(k_1 k_2 \ldots k_{n-1}, k_n) &= \gcd(m^2 + m + 1, m^2 + 3m + 3) \\ &= \gcd(m^2 + m + 1, 2m + 2) \\ &= \gcd(\frac{m}{2}(2m+2) + 1, 2m + 2) \\ &= 1\end{aligned}$$

Secondly,

$$(m^2 + m + 1)(m^2 + 3m + 3) = (m+1)^4 + (m+1)^2 + 1.$$

Problem 12. Show that, for each positive integer n, there is an n-digit number x so that the last n digits of x^2 are equal to x. (That is, $x^2 \equiv x \pmod{10^n}$.) How many of them are there?

Solution 12. Given $x^2 \equiv x \mod 10^n$, we have $x(x-1) \equiv 0 \mod 5^n$ and $x(x-1) \equiv 0 \mod 2^n$. Since x and $x - 1$ are relatively prime, 2^n and 5^n divide either x or $x - 1$, and, hence, $x \equiv 0 \mod 2^n$ or $x \equiv 1 \mod 2^n$, and, similarly, $x \equiv 0 \mod 5^n$ or $x \equiv 1 \mod 5^n$. By the Chinese Remainder Theorem, we then have 4 possibly values of x modulo 10^n.

Problem 13. Use the Jordan-Holder Theorem to prove the Fundamental Theorem of Arithmetic, which says that integers have unique prime factorization.

Solution 13. Suppose $n = p_1 \times p_2 \times \cdots \times p_k = q_1 \times q_2 \times \cdots \times q_r$ where p_i and q_i are prime for all i. Consider the two composition series

$$\{e\}, \mathbb{Z}/\left(\frac{n}{p_1 p_2 \ldots p_{k-1}}\right)\mathbb{Z}, \ldots, \mathbb{Z}/\left(\frac{n}{p_1}\right)\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$$

$$\text{and}$$
$$\{e\}, \mathbb{Z}/\left(\frac{n}{q_1 q_2 \dots q_{r-1}}\right)\mathbb{Z}, \dots, \mathbb{Z}/\left(\frac{n}{q_1}\right)\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$$

The quotients for each composition series are

$$\mathbb{Z}/p_k\mathbb{Z}, \mathbb{Z}/p_{k-1}, \dots, \mathbb{Z}/p_1\mathbb{Z}$$
$$\text{and}$$
$$\mathbb{Z}/q_r\mathbb{Z}, \mathbb{Z}/q_{r-1}, \dots, \mathbb{Z}/q_1\mathbb{Z}$$

By the Jordan-Holder theorem, we have that both composition series must be equal, and, hence, there is a bijection ϕ such that $\phi(\mathbb{Z}/p_i\mathbb{Z}) = \mathbb{Z}/q_l\mathbb{Z} \cong \mathbb{Z}/p_i\mathbb{Z} \implies p_i = q_l$. Thus, we can conclude that the q_l's are simply a rearrangement of the p_i's.

Problem 14. Show that every dihedral group D_n is solvable.

Solution 14. Consider the solvable series of D_n

$$\{e\} \to \{e, \rho, \rho^2, \rho^3, \dots, \rho^{n-1}\} \to D_n.$$

The quotients are $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

Problem 15. Show that if G is solvable and $H \leq G$, then H is solvable. Show that if G is solvable and $H \trianglelefteq G$, then G/H is solvable.

Solution 15. Let $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$ and $H = H \cap G \geq H \cap G_1 \geq H \cap G_2 \geq \cdots \geq H \cap G_n = \{e\}$. Since $G_{i+1} \trianglelefteq G_i$, we have that $H \cap G_{i+1} \trianglelefteq H \cap G_i$. Thus, the above sequence consisting of $H \cap G_i$'s becomes a normal series. Since G is solvable, we have that G_i/G_{i+1} is abelian for all i, and, hence, by constructing an injective homomorphism $f : (H \cap G_i)/(H \cap G_{i+1}) \to G_i/G_{i+1}$, we'd have that H is solvable.
Let f be defined such that $f\big(\alpha(H \cap G_{i+1})\big) = \alpha G_{i+1}$. Now, assuming $f\big(\alpha(H \cap G_{i+1})\big) = G_{i+1}$, we have that $\alpha \in G_i \implies \alpha \in H \cap G_i \implies \alpha(H \cap G_{i+1}) = H \cap G_{i+1}$. Thus, $\ker(f)$ is trivial.
Now, we may construct the solvable series $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq H \trianglerighteq \cdots \trianglerighteq G_{m-1} \trianglerighteq G_m = \{e\}$ such that G_{i+1} is a maximal subgroup of G_i. Then, we may construct the normal series $G/H \trianglerighteq G_1/H \trianglerighteq G_2/H \trianglerighteq \cdots \trianglerighteq G_n/H = \{H\}$. From Theorem 0.1.6, we have that $(G_i/H)/(G_{i+1}/H) \cong G_i/G_{i+1}$, and, hence, $(G_i/H)/(G_{i+1}/H)$ is abelian and G/H has a solvable series.

Problem 16. Suppose that $H \trianglelefteq G$, and that H and G/H are both solvable. Show that G is solvable.

Solution 16. Let $G/H \trianglerighteq G_1/H \trianglerighteq G_2/H \trianglerighteq \cdots \trianglerighteq G_n/H = \{H\}$ be a solvable series for G/H, and let $H \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \dots H_m = \{e\}$ be a solvable series for H. Then, since $(G_i/H)/(G_{i+1}/H) \cong G_i/G_{i+1}$, we know $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq H \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq \{e\}$ is a solvable series of G.

Part 2

Fields & Galois Theory

CHAPTER 2.1

Introduction To Fields

Problem 1. Prove Proposition 1.2: Let F be a field. Prove

(1) For any $a \in F$, $0 \times a = 0$.
(2) If $a, b \in F$, then $(-a)b = a(-b) = -(ab)$.
(3) $(-a)(-b) = ab$.

Solution 1. For 1, let $a \times 0 = b$. Then,

$$b = a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0 = b + b \implies b = 0.$$

For 2, we begin by noting that $(a \times -1) + a = a(-1 + 1) = a \times 0 = 0 \implies a \times -1 = -a$. Hence, by the commutativity of multiplication,

$$(-a)b = -1 \times ab = a(-1 \times b) = a(-b) = -(ab).$$

For 3, we note that $-1 \times -1 = -(-1) = 1$. Hence,

$$(-a)(-b) = -1 \times -1 \times ab = ab.$$

Problem 2. Let α be a root of $x^3 - 3x + 12$. Compute $(\alpha^2 + 2)(\alpha^2 - 2\alpha + 5)$, $\frac{1}{\alpha+1}$, and $\frac{\alpha^2+2}{\alpha^2-2\alpha+5}$ in $\mathbb{Q}(\alpha)$, by writing them in the form $a + b\alpha + c\alpha^2$, for some $a, b, c \in \mathbb{Q}$.

Solution 2. To compute $(\alpha^2 + 2)(\alpha^2 - 2\alpha + 5)$, begin by noting

$$\begin{aligned} &\implies \alpha^3 - 3\alpha + 12 = 0 \\ &\implies \alpha^3 = 3\alpha - 12 \\ &\implies \alpha^4 = 3\alpha^2 - 12\alpha \end{aligned}$$

Then,

$$\begin{aligned} (\alpha^2 + 2)(\alpha^2 - 2\alpha + 5) &= \alpha^4 - 2\alpha^3 + 7\alpha^2 - 4\alpha + 10 \\ &= 3\alpha^2 - 12\alpha - 6\alpha + 24 + 7\alpha^2 - 4\alpha + 10 \\ &= 10\alpha^2 - 22\alpha + 34 \end{aligned}$$

For the next one, note $\alpha + 1$ is a root of

$$(x - 1)^3 - 3(x - 1) + 12 = x^3 - 3x^2 + 14.$$

Hence,

$$\begin{aligned} &\implies \frac{-14}{\alpha + 1} = (\alpha + 1)^2 - 3(\alpha + 1) \\ &\implies \frac{1}{\alpha + 1} = \frac{-(\alpha + 1)^2}{14} + \frac{3(\alpha + 1)}{14} = -\frac{1}{14}\alpha^2 + \frac{1}{14}\alpha + \frac{1}{7} \end{aligned}$$

Lastly, we compute $\frac{\alpha^2+2}{\alpha^2-2\alpha+5}$ by first finding the multiplicative inverse of $\alpha^2-2\alpha+5$.

$$\begin{aligned}
&\implies (\alpha^2-2\alpha+5)(p\alpha^2+q\alpha+r)=1\\
&\implies p\alpha^4+(q-2p)\alpha^3+(r-2q+5p)\alpha^2+(5q-2r)\alpha+5r=1\\
&\implies (8p+r-2q)\alpha^2+(8q-18p-2r)\alpha+(5r-12q+24p)=1
\end{aligned}$$

Rewriting this as matrix,

$$\begin{pmatrix}5&-12&24\\-2&8&-18\\1&-2&8\end{pmatrix}\begin{pmatrix}r\\q\\p\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}\implies\begin{pmatrix}r\\q\\p\end{pmatrix}=\begin{pmatrix}\frac{7}{17}\\-\frac{1}{34}\\-\frac{1}{17}\end{pmatrix}$$

Hence,

$$\left(\alpha^2+2\right)\left(-\frac{1}{17}\alpha^2-\frac{1}{34}\alpha+\frac{7}{17}\right)=\frac{1}{34}(4\alpha^2+19\alpha+40).$$

Problem 3. Suppose K/F is an extension of fields, and $\alpha\in F$. What is the minimal polynomial of α?

Solution 3. $\{\alpha,1\}$ are linearly dependent: $\alpha-1\cdot\alpha=0$. Hence, our minimal polynomial is $x-\alpha$.

Problem 4. Show that $f:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})$ given by $f(a+b\sqrt{2})=a-b\sqrt{2}$ is an automorphism.

Solution 4. Let $\overline{a+b\sqrt{2}}=a-b\sqrt{2}$. Then, note

$$\overline{(a+b\sqrt{2})(c+d\sqrt{2})}=(ac+2bd)-(ad+bc)\sqrt{2}=\left(\overline{(a+b\sqrt{2})}\right)\left(\overline{(c+d\sqrt{2})}\right)\tag{11}$$

$$\overline{(a+b\sqrt{2})+(c+d\sqrt{2})}=(a+c)-(b+d)\sqrt{2}=\overline{(a+b\sqrt{2})}+\overline{(c+d\sqrt{2})}\tag{12}$$

$$\overline{1}=\overline{1+0\sqrt{2}}=1-0\sqrt{2}=1\tag{13}$$

From equations 11, 12, and 13, we know $f(ab)=f(a)f(b)$, $f(a+b)=f(a)+f(b)$, and $f(1)=1$. I.e. f is a homomorphism. Injectivity then follows. Lastly, f is surjective because $f(a-b\sqrt{2})=a+b\sqrt{2}$.

Problem 5. Show that there are no nontrivial automorphisms of $\mathbb{Q}(\sqrt[3]{2})$.

Solution 5. Let f be an automorphism of $\mathbb{Q}(\sqrt[3]{2})$. Firstly, note f fixes the elements of $\mathbb{Q}$ since

$$f\left(\frac{p}{q}\right)=\frac{f(p)}{f(q)}=\frac{\underbrace{f(1)+f(1)+\cdots+f(1)}_{p\text{ times}}}{\underbrace{f(1)+f(1)+\cdots+f(1)}_{q\text{ times}}}=\frac{p}{q}.$$

Hence,

$$\left(f(\sqrt[3]{2})\right)^3-2=f(0)=0.$$

Since the only root of x^3-2 in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$, we have that $f(\sqrt[3]{2})=\sqrt[3]{2}$. Then, we may conclude f is trivial by noting

$$f(a+b\sqrt[3]{2}+c\sqrt[3]{4})=f(a)+f(b)f(\sqrt[3]{2})+f(c)\left(f(\sqrt[3]{2})\right)^2=a+b\sqrt[3]{2}+c\sqrt[3]{4}.$$

Problem 6. Let x be transcendental over $\mathbb{Q}$. Why isn't there a homomorphism $f:\mathbb{Q}(x)\to\mathbb{Q}(\sqrt{2})$, obtained by "plugging in" $\sqrt{2}$ for x?

Solution 6. Suppose there was. Call this homomorphism f. We may show f fixes $\mathbb{Q}$ using the same argument we did in **Problem 5**. Then, note

$$f(x) = \sqrt{2} \implies (f(x))^2 - 2 = 0 \implies x^2 - 2 = 0.$$

Since x is transcendental, we have a contradiction.

Problem 7. Show that if $v_1, \ldots, v_n$ is a basis for a vector space V over a field F, then for every $b \in V$, there is a unique set of elements $a_1, \ldots, a_n$ of F so that $b = a_1v_1 + \cdots + a_nv_n$.

Solution 7. Since $v_1, \ldots, v_n$ is a basis, it spans V. Now, suppose $a_1v_1 + a_2v_2 + \cdots + a_nv_n = b_1v_1 + b_2v_2 + \cdots + b_nv_n$. Then,

$$(a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n = 0.$$

Since $v_1, \ldots, v_n$ are linearly independent, $a_i = b_i$ for all i $(i = 1, 2, \ldots, n)$.

Problem 8. Let V be a vector space over F, and let $a_1, \ldots, a_n$ be a linearly independent subset of V. Show that there is some basis of V that includes $a_1, \ldots, a_n$.

Solution 8. If $\{a_1, \ldots, a_n\}$ isn't already a basis, let α be a vector that can't be represented as the linear combination of $a_1, \ldots, a_n$. Append α to our set of vectors. If the set $\{a_1, \ldots, a_n, \alpha\}$ doesn't span V, repeat. Note that this only works if dim V is finite.

Alternatively, we construct our basis by appropriately replacing some other basis with the a_i's. More specifically, suppose the (infinite or finite) set $\{b_1, b_2, \ldots\}$ is a basis. Then, we write a_1 as unique combination of the b_j's. In this representation of a_1, replace a_1 with any b_j with non-zero coefficient. Notice that our new set is a basis. We do this replacement with for all a_i's, making sure not replace any a_k with some a_i. Note that this is possible because $\{a_1, \ldots, a_n\}$ are linearly independent.

Problem 9. Without using Theorem 4.3, show that if V and W are vector spaces over a field F, with $W \subseteq V$, then dim $W \leq$ dim V. Use this to prove Theorem 4.3 — any two bases of a vector space V have the same size.

Solution 9. It's odd to use the statement "dim $W \leq$ dim V" in our proof of Theorem 4.3 because, without 4.3, the definition of the dimension of a vector space doesn't make sense. Hence, we rephrase the question slightly. Suppose V has a basis of size n. Our goal is to prove all bases of W must be $\leq n$. We do this by simply noting any $n + 1$ vectors in V must be linearly dependent (Lemma 0.1.7).

Next, we prove Theorem 4.3 by first assuming there exists two bases of V of different sizes — m and n. Without loss of generality, $m > n$. By Lemma 0.1.7, the basis of size m is linearly dependent, contradicting our assumption that it's a basis.

Problem 10. Show that if $[K : F] = n$, then any $n + 1$ elements of K are linearly dependent over F.

Solution 10. See Lemma 0.1.7.

Problem 11. Show that if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ under addition and multiplication modulo p is a field, with p elements. We call this field $\mathbb{F}_p$.

Solution 11. All elements of $\mathbb{Z}/p\mathbb{Z}$ are relatively prime to p. Hence, $\mathbb{Z}/p\mathbb{Z}$ is an abelian group under addition and multiplication. Further, multiplication is distributive over addition.

Problem 12. Is $x^4 + 4$ irreducible over $\mathbb{Q}$? Prove irreducibility or find a factorization.

Solution 12. By Sophie Germain's Identity, $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$.

Problem 13. What is a 0-dimensional vector space?

Solution 13. Perhaps, it refers to the trivial vector space — $\{0\}$. $\{\}$ is our basis because 0 isn't linear independent. By convention, the empty sum $\sum_{i \in \varnothing} a_i$ is defined to be 0. Hence, we say dim $\{0\}$ is 0.

Problem 14. Show that if α is algebraic over F, then there is a unique monic polynomial $m_\alpha(x)$ of lowest degree, with coefficients in F having α as a root.

Solution 14. Let $[F(\alpha) : F] = n$. Then, consider the two monic, minimal polynomials $p(x)$ and $q(x)$, where $p(\alpha) = q(\alpha) = 0$. Note, deg $p =$ deg $q = n$. Let

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \tag{14}$$

$$q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \tag{15}$$

Then,

$$a_{n-1}\alpha^{n-1} + \cdots + a_0 = b_{n-1}\alpha^{n-1} + \cdots + b_0 \implies (a_{n-1} - b_{n-1})\alpha^{n-1} + (a_{n-2} - b_{n-2})\alpha^{n-2} + \cdots + (a_0 - b_0) = 0.$$

Since $\{\alpha^{n-1}, \alpha^{n-2}, \ldots, 1\}$ are linearly independent, $a_i = b_i$ for all i $(i = 1, 2, \ldots, n)$. I.e. $p(x) = q(x)$.

Problem 15. Let $L/K/F$ be a tower of field extensions, and let $\alpha \in L$ be algebraic over F. Let $f(x)$ be the minimal polynomial of α over F, and let $g(x)$ be the minimal polynomial of α over K. Show that $g(x)$ divides $f(x)$.

Solution 15. f is a polynomial in K with α as a root. Hence, g divides f.

Problem 16. Show that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$, by explaining how to find the multiplicative inverse of a nonzero element $a + b\sqrt[3]{2} + c\sqrt[3]{4}$.

Solution 16. Let $a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}$ be the inverse of $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Then,

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}) = (a'a + 2bc' + 2cb') + (ab' + ba' + 2cc')\sqrt[3]{2} + (ac' + bb' + ca')\sqrt[3]{4} = 1.$$

Rewriting this as a matrix, we have

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

For notational convenience, let

$$A = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

We call the determinant of A det. Then,

$$\det = a(a^2 - 2bc) - 2c(ab - 2c^2) + 2b(b^2 - ac) = a^3 + 2b^3 + 4c^3 - 6abc.$$

Before computing A^{-1}, we show det is nonzero whenever either a,b, or c are nonzero. Since a, b, and c are rational, we set

$$a = \frac{p}{q}$$
$$b = \frac{p'}{q'}$$
$$c = \frac{p''}{q''}$$

Then,

$$\det = 0 \implies (pq'q'')^3 + 2(p'qq'')^3 + 4(p''q'q)^3 - 6pp'p''(qq'q'')^2 = 0.$$

Setting $u = pq'q''$, $v = p'qq''$, and $w = p''q'q$, we have that $u^3 + 2v^3 + 4w^3 - 6uvw = 0$ — the same equation as our first one, but now our variables are in $\mathbb{Z}$. Hence, by Lemma 0.1.8, the only solution is when $u = v = w = 0$, which is precisely when $a = b = c = 0$. Now, with some help from Wolfram Alpha,

$$a' = \frac{a^2 - 2bc}{\det}$$
$$b' = \frac{2c^2 - ab}{\det}$$
$$c' = \frac{b^2 - ac}{\det}$$

Problem 17. Show that if α and β are algebraic over F , then $\alpha + \beta$ and $\alpha\beta$ are also algebraic over F. Find a nonzero polynomial with coefficients in $\mathbb{Q}$ that has $\sqrt{2} + \sqrt[3]{3}$ as a root.

Solution 17. We prove a slight stronger statement — $F(\alpha, \beta)$ is an algebraic extension of F. Let the degree of the minimum polynomials of α and β be n and m respectively. Then, by the Tower Law,

$$[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)] \times [F(\alpha) : F].$$

$[F(\alpha)(\beta) : F(\alpha)] \leq m$ and $[F(\alpha) : F] = n$. Hence, $[F(\alpha, \beta) : F] \leq mn$.

Lastly, consider the polynomial $f(x) = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$. For this f, $f(\sqrt{2} + \sqrt[3]{3}) = 0$. We find f as follows:

$$\implies x - \sqrt{2} - \sqrt[3]{3} = 0$$
$$\implies (x - \sqrt{2})^3 = 3$$
$$\implies x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} - 3 = 0$$
$$\implies (x^3 + 6x - 3)^2 = 2(3x^2 + 2)^2 \implies x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0$$

Problem 18. Prove Theorem 6.6 — Eisenstein's Criterion.

Solution 18. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Z}$, $p \nmid a_n$, $p \mid a_{n-1}, a_{n-2}, \ldots, a_0$, and $p^2 \nmid a_0$ for some prime p. Note f is irreducible over $\mathbb{Q}$ if and only if f is irreducible over $\mathbb{Z}$ (By Gauß's Lemma). Now, suppose f is reducible over $\mathbb{Z}$. I.e.

$$f(x) = (p_m x^m + p_{m-1}x^{m-1} + \cdots + p_0)(q_r x^r + q_{r-1}x^{r-1} + \cdots + q_0)$$

where $p_i, q_j \in \mathbb{Z}$ $(i = 0, 1, \ldots, m \ \& \ j = 0, 1, \ldots, r)$. Since $p \mid a_0 = p_0 q_0$ but $p^2 \nmid a_0$, we have that either $p \mid p_0$ or $p \mid q_0$ (not both). WLOG, suppose $p \mid p_0$. We prove by induction that $p \mid p_i$ for all i. Then, assume $p \mid p_k$ for all $k \leq i$. Since deg f is greater than the degree of its factors, $i + 1 \neq n$. Then, we have that

$$a_{i+1} = p_{i+1}q_0 + p_i q_1 + \cdots \equiv 0 \pmod{p} \implies p_{i+1}q_0 \equiv 0 \pmod{p} \implies p | p_{i+1}.$$

We then contradict our assumption that $p \nmid a_n = p_n q_n$.

Problem 19. Show that if p is a prime, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, and a_n is not divisible by p, then if the reduction of $f(x)$ modulo p is irreducible over $\mathbb{F}_p$, then $f(x)$ is irreducible over $\mathbb{Q}$. (You may assume Gauß's Lemma, which says that if a polynomial with integer coefficients factors into two polynomials with rational coefficients, it also factors into two polynomials with integer coefficients). Apart from Eisenstein's Criterion, this is the main way of proving irreducibility of polynomials.

Solution 19. We prove the contrapositive. Suppose $f(x) = g(x)h(x)$ where

$$g(x) = \alpha_p x^p + \alpha_{p-1}x^{p-1} + \cdots + \alpha_0$$
$$h(x) = \beta_q x^q + \beta_{q-1}x^{q-1} + \cdots + \beta_0$$

Note that the α_i's and β_j's are integers. Call the reduction of f,g, and h modulo p f', g', and h'. Then, $f'(x) \equiv g'(x)h'(x) \pmod{p}$. Since $p \nmid a_n$, $p \nmid \alpha_p$ and $p \nmid \beta_q$. Hence, neither g' nor h' are constant polynomials.

Problem 20. Show that if F is a field with finitely many elements, then the number of elements is a power of a prime.

Solution 20. Consider the additive group of F — G. Let $\alpha, \beta \in G$. Then, consider the automorphism $f : G \to G$ where $f(x) = kx$ $(k \neq 0)$.

(Homomorphism) $f(x + y) = k(x + y) = kx + ky = f(x) + f(y)$

(Injectivity) $kx = ky \implies x = y$

(Surjectivity) $z = f(x) \implies x = k^{-1}z$

Setting $k = \beta\alpha^{-1}$, we have a homomorphism that maps α to β. Hence, $|\alpha| = |\beta|$. By Cauchy's Theorem, G must then be of prime power order.

Problem 21. Describe a field with exactly 4 elements.

Solution 21. The splitting field of $x^2 + x + 1$ over $\mathbb{F}_2$: $\mathbb{F}_2\left(\frac{1+\sqrt{3}i}{2}\right)$.

Problem 22. Show that if α is an irrational number which is the root of a polynomial f of degree n, then there exists a real number $C > 0$ such that, for all integers p, q

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}.$$

(Hint: Mean Value Theorem.) This is a theorem of Liouville. (One might say, the "other" theorem of Liouville, thanks to his more famous theorem in complex analysis).

Solution 22. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. We prove $C = \min\left(c, \frac{1}{K}\right)$ where c is some positive element of $\mathbb{R}$ such that f has no roots in $[\alpha - c, \alpha + c]$ other than α and $K > \max(|f'(x)|)$ for $x \in [\alpha - c, \alpha + c]$. When q^n is negative, our result is apparent. Hence, we consider the case where $q^n > 0$. Now, suppose there

exists p and q such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{c}{q^n}.$$

Then, $\alpha - c \leq \frac{p}{q} \leq \alpha + c$. By the Mean Value Theorem, there exists x such that

$$\frac{f(p/q)}{p/q - \alpha} = f'(x) \implies |p/q - \alpha| = \left|\frac{f(p/q)}{f'(x)}\right| = \frac{1}{q^n}\left|\frac{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n}{f'(x)}\right| > \frac{1}{Kq^n}.$$

Problem 23. Show that $\sum_{i=1}^{\infty} 10^{-i!}$ is transcendental. This was the first number (or, rather, a member of the first family of numbers) proven to be transcendental.

Solution 23. Let $\alpha = \sum_{i=1}^{\infty} 10^{-i!}$. Since the decimal representation of α is non-terminating and non-recurring, α is irrational. Now, supposes α is algebraic. Then, there exists C and n such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$$

for all $p/q \in \mathbb{Q}$. Let $\frac{p}{q} = \sum_{i=1}^{m} 10^{-i!}$ and $q = 10^{m!}$. Then,

$$q^n\left(\alpha - \frac{p}{q}\right) = q^n \sum_{i=m+1}^{\infty} 10^{-i!} = \sum_{i=m+1}^{\infty} 10^{(m!\cdot n)-i!} > C.$$

We prove $\lim_{m\to\infty} \sum_{i=m+1}^{\infty} 10^{(m!\cdot n)-i!} = 0$ by showing each individual summand goes to 0. Let the limit of the kth summand be

$$L = \lim_{m\to\infty} 10^{(m!\cdot n)-(m+k)!}.$$

Begin by choosing m such that $(m+k)(m+k-1)\ldots(m+1) > n$. For such m, $10^{(m!\cdot n)-(m+k)!} < 1$. Then,

$$0 < 10^{\left((m+1)!\cdot n\right)-(m+k+1)!} = \frac{(10^{m!\times n})^{m+1}}{(10^{(m+k)!})^{m+k+1}} < 10^{(m!\cdot n)-(m+k)!}.$$

Hence, our limit exists. Then,

$$\log_{10}(L) = (m!\cdot n) - (m+k)! \to -\infty \text{ as } m \to \infty \implies L \to 0.$$

CHAPTER 2.2

Constructibility and Galois Groups

Problem 1. Show that, for any positive integer n, it is possible to divide a line segment into n equal pieces using a compass and straightedge.

Solution 1.

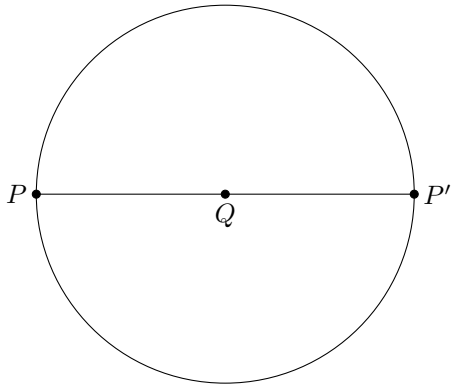


FIGURE 1. Given points P and Q, we construct a point P' on line PQ such that $|PQ| = |P'Q|$

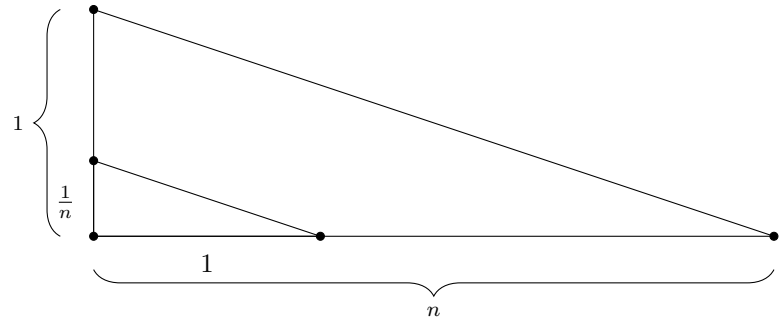


FIGURE 2. Given segments of length 1 and n ($\mathbb{Z}$ is constructible), we construct a segment of length $1/n$

Problem 2. Show that it is impossible to construct a regular heptagon (7-gon) or nonagon (9- gon) using straightedge and compass.

Solution 2. Suppose we could construct a 9-gon. In doing so, we would construct an angle of $\frac{7\pi}{9}$. Let $\theta = \frac{7\pi}{9}$. Then, by the triple angle identity of cos,

$$4\cos^3(\theta) - 3\cos(\theta) = \cos(7\pi/3) \implies 4\cos^3(\theta) - 3\cos(\theta) - \frac{1}{2} = 0.$$

Having proven this polynomial is irreducible, we may conclude $[\mathbb{Q}(\theta) : \mathbb{Q}]$ is not a power of 2.

Next, suppose we could construct a 7-gon. We separate it into 7 congruent triangles — each of which have exactly one angle of $\frac{2\pi}{7}$. Notice $\frac{2\pi}{7}$ is a root of

$$\cos(4x) - \cos(3x) = (\cos(x) - 1)(-1 - 4\cos(x) + 4\cos^2(x) + 8\cos^3(x))$$

and $\cos\left(\frac{2\pi}{7}\right)$ is a root of $8x^3 + 4x^2 - 4x - 1$. By Lemma 0.1.11, our cubic has no roots in $\mathbb{Q}$ and, hence, must be irreducible. Then, $[\mathbb{Q}(\cos\left(\frac{\pi}{7}\right)) : \mathbb{Q}]$ is not a power of 2.

Problem 3. Explain how to construct a regular pentagon using straightedge and compass. (Possible hint: what is $\cos(\frac{2\pi}{5})$ in terms of radicals?)

Solution 3.

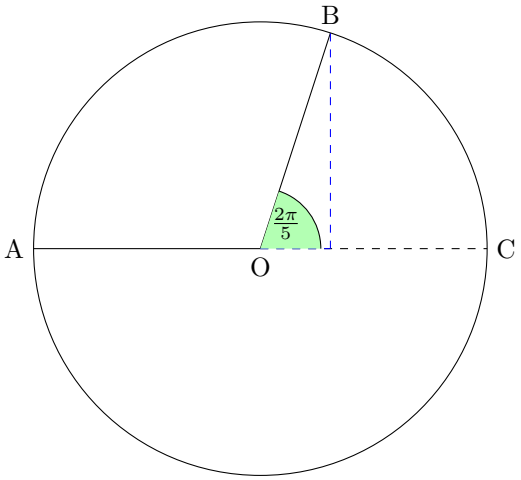


FIGURE 3. Partially Complete Pentagon

Notice that we need only prove $\cos\left(\frac{2\pi}{5}\right)$ is constructible. Note that

$$\cos\left(\frac{4\pi}{5}\right) = \cos\left(2\pi - \frac{4\pi}{5}\right) = \cos\left(\frac{6\pi}{5}\right).$$

Hence, $\frac{2\pi}{5}$ is a root of

$$\cos(3x) - \cos(2x) = 4\cos^3(x) - 2\cos^2(x) - 3\cos(x) + 1$$

and $\cos(\frac{2\pi}{5})$ is a root of $4x^3 - 2x^2 - 3x + 1$.

$$4x^3 - 2x^2 - 3x + 1 = 0 \implies x \in \left\{1, \frac{\sqrt{5}-1}{4}, \frac{-(\sqrt{5}+1)}{4}\right\}$$

Hence, $\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$.

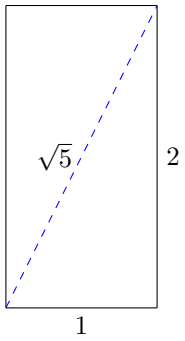


FIGURE 4. Constructing $\sqrt{5}$

Seeing as the set of constructible numbers is closed under addition and multiplication, $\frac{\sqrt{5}-1}{4}$ is constructible.

Problem 4. Show that it is possible to trisect an angle using a marked ruler and compass. (A marked ruler has two marked points on it, so that the distance between them is 1).

Solution 4.

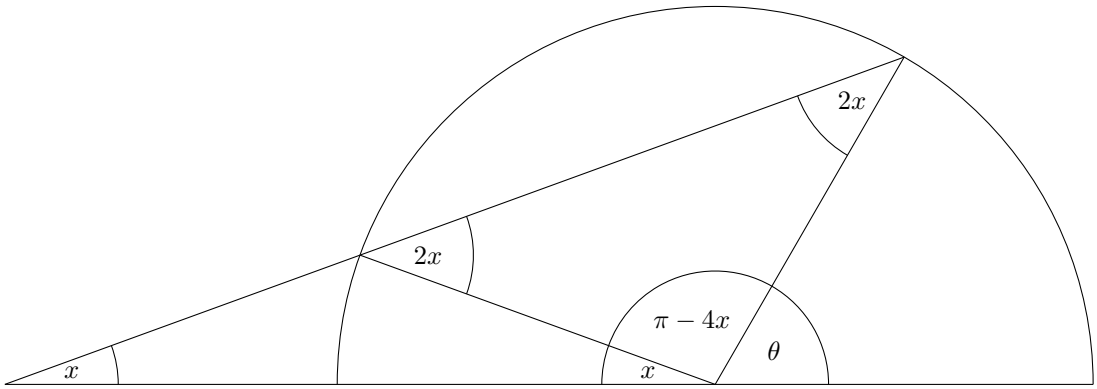


FIGURE 5. Archimedes Construction
Notice that $x + \pi - 4x + \theta = \pi \implies x = \theta/3$.

Problem 5. Let K/F be a field extension, and suppose that $g_1, \ldots, g_n \in \mathrm{Aut}(K/F)$. Show that $K^{\{g_1,\ldots,g_n\}} = K^{\langle g_1,\ldots,g_n\rangle}$. (In other words, the subfield fixed by $g_1, \ldots, g_n$ is equal to the subfield fixed by the group generated by $g_1, \ldots, g_n$.

Solution 5.

- $\{g_1, \ldots, g_n\} \subseteq \langle g_1, \ldots, g_n\rangle$ implies $K^{\langle g_1,\ldots,g_n\rangle} \leq K^{\{g_1,\ldots,g_n\}}$.
- Elements fixed by $\{g_1, \ldots, g_n\}$ (elements of $K^{\{g_1,\ldots,g_n\}}$) are fixed by all compositions of $\{g_1, \ldots, g_n\}$ (elements of $\langle g_1, \ldots, g_n\rangle$). I.e. $K^{\{g_1,\ldots,g_n\}} \leq K^{\langle g_1,\ldots,g_n\rangle}$.

Problem 6. Show that $\mathbb{C}/\mathbb{R}$ is a Galois extension. What is its Galois group?

Solution 6.

- Consider the automorphism $f : \mathbb{C} \to \mathbb{C}$ such that $f(a + bi) = a - bi$. Only $\mathbb{R}$ is fixed.

- $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Problem 7. Is $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ a Galois extension? What about $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$?

Solution 7. $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ consists of only the identity and the automorphism $f : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ such that $f(\sqrt[4]{2}) = -\sqrt[4]{2}$.

$$f\left(a + b\sqrt[4]{2} + c(\sqrt[4]{2})^2 + d(\sqrt[4]{2})^3\right) = a + b\sqrt[4]{2} + c(\sqrt[4]{2})^2 + d(\sqrt[4]{2})^3 \implies b = d = 0.$$

Notice that the identity fixes all of $\mathbb{Q}(\sqrt[4]{2})$ and f fixes all elements of the form $a + b\sqrt{2}$. Hence, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ isn't Galois. Similarly, $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$ consists of only the identity and the automorphism $f : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ such that $f(\sqrt[4]{2}) = -\sqrt[4]{2}$.

$$f(a\sqrt[4]{2} + b) = a\sqrt[4]{2} + b \implies a = 0.$$

Since f only fixes $\mathbb{Q}(\sqrt{2})$, our extension is Galois.

Problem 8. Suppose that $L/K/F$ is a tower of field extensions. Show that if L/F is Galois, then L/K is Galois. Give an example to show that K/F is not necessarily Galois.

Solution 8. We employ the following definition of a Galois Extension:

$$K/F \text{ is Galois if and only if } K/F \text{ is normal and separable.}$$

Now, suppose L/F was normal. I.e. $L = F(\alpha_1, \alpha_2, \dots)$. In our (finite or infinite) sequence of α_i's, suppose $\beta_1, \beta_2, \dots \notin K$. Then, $L = K(\beta_1, \beta_2, \dots)$. Next, suppose L/K wasn't separable. I.e. there exists α in L with minimal polynomial f in K such that $f'(\alpha) = 0$. Let the minimal polynomial of α in F be g. Since $f|g$, there exists k such that

$$g(x) = f(x)k(x) \implies g'(\alpha) = f'(\alpha)k'(\alpha) = 0.$$

Problem 9. If L/K and K/F are Galois, is L/F necessarily Galois? Prove or give a counterexample.

Solution 9. Counterexample: $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Problem 10. Determine the splitting fields and their degrees over Q for the following polynomials:

(a) $x^4 - 2$
(b) $x^4 + 2$
(c) $x^4 + 4$
(d) $x^3 - x^2 - 2x + 1$

Solution 10.

(a) $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$. $[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}] = 8$.
(b) $\mathbb{Q}\left(\sqrt[4]{2}e^{i\pi/4}, \sqrt[4]{2}e^{3i\pi/4}\right)$. $[\mathbb{Q}\left(\sqrt[4]{2}e^{i\pi/4}, \sqrt[4]{2}e^{3i\pi/4}\right) : \mathbb{Q}] = 8$.
(c) $\mathbb{Q}(i)$. $[\mathbb{Q}(i) : \mathbb{Q}] = 2$
(d) Call the splitting field K. Then, $[K : \mathbb{Q}] = 3$

Problem 11. What is the Galois Group of $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$? Determine all the subgroups of this Galois group and compute their fixed fields.

Solution 11. $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}\right) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$$\begin{aligned}
\sigma_1(\sqrt{2}) &= \sqrt{2} & \sigma_1(\sqrt{3}) &= \sqrt{3} \\
\sigma_2(\sqrt{2}) &= -\sqrt{2} & \sigma_2(\sqrt{3}) &= \sqrt{3} \\
\sigma_3(\sqrt{2}) &= \sqrt{2} & \sigma_3(\sqrt{3}) &= -\sqrt{3} \\
\sigma_4(\sqrt{2}) &= -\sqrt{2} & \sigma_4(\sqrt{3}) &= -\sqrt{3}
\end{aligned}$$

Then,

$$\begin{aligned}
\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)^{\{\sigma_1\}} &= \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \\
\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)^{\{\sigma_1,\sigma_2\}} &= \{x \in \mathbb{Q}(\sqrt{2},\sqrt{3}) |\ x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ b = d = 0\} = \mathbb{Q}(\sqrt{3}) \\
\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)^{\{\sigma_1,\sigma_3\}} &= \{x \in \mathbb{Q}(\sqrt{2},\sqrt{3}) |\ x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ c = d = 0\} = \mathbb{Q}(\sqrt{2}) \\
\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)^{\{\sigma_1,\sigma_4\}} &= \{x \in \mathbb{Q}(\sqrt{2},\sqrt{3}) |\ x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ b = c = 0\} = \mathbb{Q}(\sqrt{6})
\end{aligned}$$

Problem 12. What is the automorphism group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$? Determine all the subgroups of this automorphism group, and compute their fixed fields.

Solution 12. $\mathrm{Gal}\left(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\right) = \{\sigma_1, \sigma_2\} \cong \mathbb{Z}/2\mathbb{Z}$.

$$\begin{aligned}
\sigma_1(\sqrt[4]{2}) &= \sqrt[4]{2} & \sigma_2(\sqrt[4]{2}) &= -\sqrt[4]{2} \\
\mathbb{Q}(\sqrt[4]{2})^{\{\sigma_1\}} &= \mathbb{Q}(\sqrt[4]{2}) & \mathbb{Q}(\sqrt[4]{2})^{\{\sigma_1,\sigma_2\}} &= \mathbb{Q}(\sqrt{2})
\end{aligned}$$

Problem 13. Suppose that $f(x)$ is a separable polynomial of degree $n > 0$ with coefficients in a field F, and let K be the splitting field. Show that there is an injective homomorphism $\phi : \mathrm{Gal}(K/F) \to S_n$.

Solution 13. Call the n distinct roots of f $\alpha_1, \ldots, \alpha_n$. Notice that the elements of $\mathrm{Gal}(K/F)$ are defined by how they permute $\alpha_1, \ldots, \alpha_n$. For $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$, $\sigma_1(\alpha_p) = \alpha_q$ and $\sigma_2(\alpha_q) = \alpha_r$. Then, we define our map $\phi : \mathrm{Gal}(K/F) \to S_n$ such that $\phi(\sigma_1)(p) = q$. Note ϕ is a homomorphism since

$$\phi(\sigma_2\sigma_1)(p) = r = (\phi(\sigma_2)\phi(\sigma_1))\,(p).$$

Problem 14. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is a separable polynomial with coefficients in a field F. Suppose that, over the splitting field, we have $f(x) = \prod_{i=1}^{n}(x - r_i)$. We define its discriminant to be

$$\mathrm{Disc}(f) = \prod_{\substack{1 \le i,j \le n \\ i<j}} (r_i - r_j)^2.$$

Show that $\mathrm{Disc}(f) \in F$. Show that, under the homomorphism from **Problem 13**, if $\mathrm{Disc}(f)$ is a perfect square in F, then $\mathrm{im}(\phi) \le A_n$.

Solution 14. Call the splitting field of f over F K. By Lemma 0.1.14, K is Galois. Hence, $\mathrm{Disc}(f) \in F$ because it is fixed by $\mathrm{Gal}(K/F)$. If $\mathrm{Disc}(f)$ is a perfect square, then

$$\prod_{\substack{1 \le i,j \le n \\ i<j}} (r_i - r_j)$$

is fixed by $\mathrm{Gal}(K/F)$. Suppose there exists an odd automorphism σ in $\mathrm{Gal}(K/F)$. Then,

$$\prod_{\substack{1\le i,j\le n\\ i<j}}(r_i-r_j)=\sigma\left(\prod_{\substack{1\le i,j\le n\\ i<j}}(r_i-r_j)\right)=-1\times\prod_{\substack{1\le i,j\le n\\ i<j}}(r_i-r_j).$$

Assuming $1\neq -1$ in F, we have a contradiction.

Comment. Notice that for an arbitrary polynomial or field, $\mathrm{Disc}(f)$ being a perfect square doesn't imply $\mathrm{im}(\phi)\le A_n$. Consider x^2+x+1 in $\mathbb{F}_2$ — a field where $1=-1$. Here, $\mathrm{im}(\phi)=S_2$ even though $\mathrm{Disc}(F)=1$ is a perfect square. If we restrict our choice of F to those where $1\neq -1$, everything works as expected.

Problem 15. Show that if K/F is an algebraic extension with $K^{\mathrm{Aut}(K/F)}=F$, then K/F is normal and separable. (Hint: Pick some $\alpha\in K$ and look at the polynomial whose roots are $\sigma(\alpha)$ for $\sigma\in\mathrm{Aut}(K/F)$).

Solution 15. Let the roots of $m_\alpha(x)$ (the minimal polynomial of α over F) in K be $\alpha_1,\alpha_2,\ldots,\alpha_m$. Notice

$$S=\left\{\prod_i^m\alpha_i\ ,\ \sum_{j_1<\cdots<j_{m-1}}\prod_{i=1}^{m-1}\alpha_{j_i}\ ,\ \ldots\ ,\ \sum_{j_1<j_2}\prod_{i=1}^{2}\alpha_{j_i}\ ,\ \sum_i^m\alpha_i\ ,\ 1\right\}$$

is fixed by $\mathrm{Gal}(K/F)$ and, hence, belongs in F. By Vieta's formula, the elements of S are coefficient of $m_\alpha(x)$. Then, $m_\alpha(x)$ is separable and splits into linear factors over K. I.e. K/F is normal and separable.

Problem 16. Show that, if p is a prime, then the so-called pth cyclotomic polynomial $x^{p-1}+x^{p-2}+\cdots+x+1$ is irreducible.

Solution 16. Consider a variant of pth cyclotomic polynomial

$$(x+1)^{p-1}+(x+1)^{p-1}+(x+1)^{p-2}+\cdots+(x+1)+1.$$

We choose to work with this because it's in Eisenstein form. Let the coefficient of the x^i term be a_i. Then, we find that

$$a_i=\binom{i}{i}+\binom{i+2}{i}+\cdots+\binom{p-1}{i}.$$

By Lemma 0.1.10, $a_i=\binom{p}{i+1}$. We can now see that $a_0=p$, $a_{p-1}=1$, and p divides all other a_i's. Our polynomial must then be irreducible.

Problem 17. The n^{th} cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial

$$\Phi_n(x)=\prod_{\substack{1\le a\le n\\ \gcd(a,n)=1}}(x-e^{2\pi ia/n}).$$

In other words, the roots are the n^{th} roots of unity which are not m^{th} roots of unity for any $m<n$. Show that

$$x^n-1=\prod_{d\mid n}\Phi_d(x).$$

Solution 17. Note that $\Phi_d(x)\mid x^n-1$ given $d\mid n$ and $\deg\Phi_d(x)=\phi(d)$. Then, note $\Phi_\alpha(x)$ shares no roots with $\Phi_\beta(x)$ if $\alpha\neq\beta$. By Lemma 0.1.16, our result follows.

Problem 18. Show that $\Phi_n(x)$ has integral coefficients.

Solution 18. Suppose there exists some $\Phi_n(x)$ with non-integral coefficients. Let n be the smallest natural number for this to be true. Then, by **Problem 19**,

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

Notice both $\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)$ and $x^n - 1$ belong in $\mathbb{Z}[X]$ and have leading coefficient 1. By Lemma 0.1.15, we have a contradiction.

Problem 19. Show that $\Phi_n(x)$ is irreducible. (Reduce modulo p, for some $p \nmid n$.) Conclude that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Solution 19. Let f be the minimal polynomial of ζ_n. We prove $f(\zeta_n^p) = 0$ for prime p ($p \nmid n$). Let $\Phi_n(x) = f(x)g(x)$. Suppose $g(\zeta_n^p) = 0$. Then, note $f(x) \mid g(x^p)$. Now, consider the reduction of our polynomials modulo p. Let

$$f \equiv f' \pmod{p}$$
$$g \equiv g' \pmod{p}$$

Then, note $f'(x) \mid g'(x^p) = (g'(x))^p \implies f' | g'$ by Lemma 0.1.17. Since $x^n - 1$ has no repeated roots modulo p, we have a contradiction. Note that by repeated use of this argument, we can show $f(\zeta_n^{p_1 p_2 \cdots p_m}) = 0$ for primes p_i $(i = 1, 2, \ldots, m)$ that don't divide n. Thus, $\Phi_n(x) \mid f$ and $f = \Phi_n(x)$. It follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Problem 20. Determine the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Is it isomorphic to a familiar group?

Solution 20. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Consider the map $f : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ such that, given $\sigma(\zeta_n) = \zeta_n^a$, $f(\sigma) = a$.

Problem 21.

(1) Suppose that $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Show that if $x \geq 0$, then $\sigma(x) \geq 0$.
(2) For any rational $\epsilon > 0$, show that if $|a - b| < \epsilon$, then $|\sigma(a) - \sigma(b)| < \epsilon$.
(3) Show that $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{e\}$.

Solution 21.

(1) Given $x \geq 0$, there exists y such that $x = y^2$. Then, $\sigma(x) = \sigma(y^2) = (\sigma(y))^2 \geq 0$.
(2) Suppose $-\epsilon < a - b < \epsilon$. Then, by part (1), $b - a + \epsilon > 0 \implies \sigma(a) - \sigma(b) < \epsilon$ and $a - b + \epsilon > 0 \implies \sigma(a) - \sigma(b) > -\epsilon$.
(3) Let $\alpha \in \mathbb{R}$ be irrational and $\sigma(\alpha) = \beta$ where $\alpha \neq \beta$. By the density of $\mathbb{Q}$ in $\mathbb{R}$, choose some p, ϵ in $\mathbb{Q}$ such that $|\alpha - p| < \epsilon$ and $\epsilon < \frac{|\alpha - \beta|}{2}$. By part (2), we have that $|\sigma(\alpha) - p| < \epsilon$. Then, notice that $\sigma(\alpha) \neq \beta$ — contradiction.

CHAPTER 2.3

The Galois Correspondence

Problem 1. Show that if r is a factor of $2^{2^n}+1$, then $r \equiv 1 \pmod{2^{n+1}}$.

Solution 1. Let p (a prime) divide $2^{2^n}+1$. I.e. $2^{2^n} \equiv -1 \pmod{p}$. We know there exists an element g with $|g| = p-1$. Then, let $g^a \equiv 2 \pmod{p}$ and, hence,

$$\begin{aligned}
&\implies g^{a2^n} \equiv -1 \pmod{p} \\
&\implies a2^n = k(p-1) + \frac{p-1}{2} \\
&\implies a2^{n+1} = (2k+1)(p-1) \\
&\implies p \equiv 1 \pmod{2^{n+1}}.
\end{aligned}$$

It follows that $r \equiv 1 \pmod{2^{n+1}}$.

Problem 2. Show that

$$\cos\left(\frac{2\pi}{17}\right) = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{16}.$$

Solution 2. Note that $\cos(18\pi/17) = \cos(16\pi/17)$. Then, $\frac{2\pi}{17}$ is a root of

$$\begin{aligned}
&= \cos(9x) - \cos(8x) \\
&= 256\cos^9(x) - 128\cos^8(x) - 576\cos^7(x) + 256\cos^6(x) + 432\cos^5(x) \\
&\quad - 160\cos^4(x) - 120\cos^3(x) + 32\cos^2(x) + 9\cos(x) - 1 \\
&= (256\cos^8(x) + 128\cos^7(x) - 448\cos^6(x) - 192\cos^5(x) \\
&\quad + 240\cos^4(x) + 80\cos^3(x) - 40\cos^2(x) - 8\cos(x) + 1)\,(\cos(x) - 1)
\end{aligned}$$

and $2\cos\left(\frac{2\pi}{17}\right)$ is a root of

$$f(x) = x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1.$$

With some computation, we can show

$$f\left(\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{8}\right) = 0.$$

Now, notice that for all $x > 1.73$, $f'(x)$ is positive since

$$f'(x+1.73) = 8x^7 + 103.88x^6 + 533.467x^5 + 1370.72x^4 + 1828.35x^3 + 1171.96x^2 + 272.27x + 0.97258$$

has positive coefficients. Then, since $2\cos(2\pi/17) > 2\cos(\pi/6) = \sqrt{3} > 1.73$ and

$$\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{8} \approx 1.864944\ldots,$$

our result follows.

Problem 3. Let K be the splitting field over $\mathbb{Q}$ of $x^4 - 7$. Write down all the intermediate subfields F and compute the Galois groups $\mathrm{Gal}(K/F)$. For which intermediate fields F is $F/\mathbb{Q}$ Galois?

Solution 3. Note $\mathrm{Gal}(K/F) \cong D_4$ and generated by

$$\begin{array}{llll} \rho(\sqrt[4]{7}) = \sqrt[4]{7}i & \rho(-\sqrt[4]{7}) = -\sqrt[4]{7}i & \rho(\sqrt[4]{7}i) = -\sqrt[4]{7} & \rho(-\sqrt[4]{7}i) = \sqrt[4]{7} \\ \tau(\sqrt[4]{7}) = -\sqrt[4]{7}i & \tau(-\sqrt[4]{7}) = \sqrt[4]{7}i & \tau(\sqrt[4]{7}i) = -\sqrt[4]{7} & \tau(-\sqrt[4]{7}i) = \sqrt[4]{7} \end{array}$$

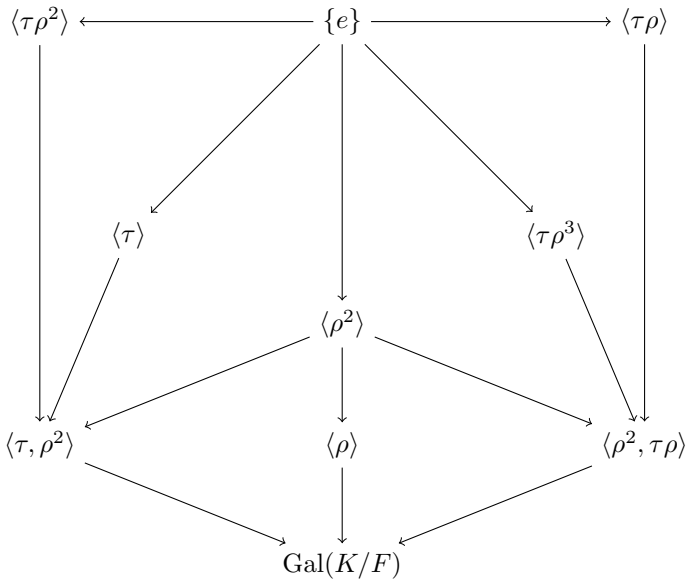


FIGURE 1. Subgroups of $\mathrm{Gal}(K/F)$

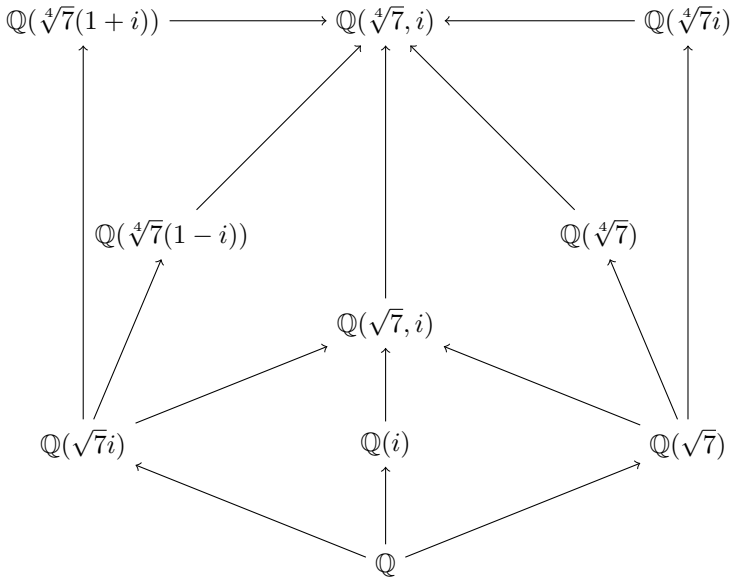


FIGURE 2. Intermediate Subfields of K/F

Note that the only intermediate field extensions $F/\mathbb{Q}$ that are normal (and hence Galois) are $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{7}i)/\mathbb{Q}$, and $\mathbb{Q}(\sqrt{7}, i)/\mathbb{Q}$.

Problem 4. If $N/K/F$ and $N/L/F$ are towers of field extensions, let KL denote the smallest subfield of N containing both K and L. Show that if K/F and L/F are Galois extensions, then KL/F is Galois as well, and that there is an injective homomorphism $\phi : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$. If $K \cap L = F$, show that ϕ is an isomorphism.

Solution 4. Let K be the splitting field of the set of polynomials S_α and L be the splitting of the set of polynomials S_β over F. Then, KL is the splitting field of $S_\alpha \cup S_\beta$. It follows that KL is separable since the elements of S_α and S_β are separable. Now, we define our homomorphism ϕ such that $\phi(\psi) = (\psi_1, \psi_2)$ where $\psi(i) = \psi_1(i),\ \forall i \in K$ and $\psi(j) = \psi_2(j),\ \forall j \in L$. Suppose $\phi(x) = (\sigma_x, \tau_x)$ and $\phi(y) = (\sigma_y, \tau_y)$.

$$\text{(Homomorphism)} \qquad \phi(xy) = (\sigma_x \circ \sigma_y, \tau_x \circ \tau_y) = (\sigma_x, \tau_x)(\sigma_y, \tau_y) = \phi(x)\phi(y)$$

$$\text{(Injectivity)} \qquad \phi(x) = \phi(y) \implies \sigma_x = \sigma_y \ \&\ \tau_x = \tau_y \implies x = y$$

Note that for our injectivity argument, we use that x and y permute the basis in the same way iff $x = y$. To prove $[KL : F] = [K : F] \times [L : F]$ given $K \cap L = F$, we use a result from **Problem 2** of the following chapter. In particular,

$$[KL : L] = [K : K \cap L] \implies [KL : F] = [KL : L] \times [L : F] = [K : K \cap L] \times [L : F] = \frac{[K : F] \times [L : F]}{[K \cap L : F]}.$$

Problem 5. Show that if K/F and L/F are Galois extensions, $[K : F]$ and $[L : F]$ are relatively prime, then $\mathrm{Gal}(KL/F) \cong \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$

Solution 5. Since $[K : F]$ and $[L : F]$ are relatively prime, $[K \cap L : F] = 1 \implies K \cap L = F$. By **Problem 5**, the result follows.

Problem 6. Show that if K/F is a Galois extension and L/F is an arbitrary extension, then KL/L is a Galois extension, and that there is an injective homomorphism $\mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$.

Solution 6. Call set of polynomials for which K is a splitting of F S. Then, KL is the splitting of S over L. Since the elements of S are separable, we have that KL/L is Galois. Note the elements of $\mathrm{Gal}(KL/L)$ fix F and send K to K. Then, we define our homomorphism $\phi : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ such that $\phi(\tau) = \sigma$ where $\tau(i) = \sigma(i),\ \forall i \in K$.

Problem 7. Let K be the splitting field of $f(x) = x^5 - 2$. Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ by writing down what all the automorphisms look like. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is generated by two elements σ and τ, with $\sigma^5 = e$ and $\tau^4 = e$ and $\tau\sigma\tau^{-1} = \sigma^2$. This group is called F_5, where the "F" stands for Frobenius.

Solution 7. Begin by noting $K = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$ and, hence, $[K : \mathbb{Q}] = 4 \times 5 = 20$. Now, label the roots

$$a_1 = \sqrt[5]{2} \qquad a_4 = \sqrt[5]{2}\zeta_5^3$$
$$a_2 = \sqrt[5]{2}\zeta_5 \qquad a_5 = \sqrt[5]{2}\zeta_5^4$$
$$a_3 = \sqrt[5]{2}\zeta_5^2$$

We need only prove the permutations $\sigma = (12345)$ and $\tau = (2354)$ belong in the image of the map $\mathrm{Gal}(K/F) \to S_5$, verify that

$$\begin{aligned} \sigma^5 &= (12345)^5 = e \\ \tau^4 &= (2354)^4 \\ \tau\sigma\tau^{-1} &= (2354)(12345)(2453) = (35241) = \sigma^2 \end{aligned}$$

and note that $\sigma^a\tau^b = 0 \iff a \equiv b \equiv 0 \pmod 5$ (powers of σ are always 5-cycles and powers of τ always fix 1). It then follows that our Galois Group is F_5.

	σ	σ^2	σ^3	σ^4	σ^5
τ	(1325)	(1534)	(1243)	(1452)	(2354)
τ^2	(15)(24)	(14)(23)	(13)(45)	(12)(35)	(25)(34)
τ^3	(1435)	(1254)	(1523)	(1342)	(2453)
τ^4	(12345)	(35241)	(14253)	(15432)	e

FIGURE 3. Elements of $\mathrm{Gal}(K/\mathbb{Q})$

Problem 8. Let $f(x)$ be an irreducible, separable polynomial over a field F, and let L be its splitting field. Suppose that K is an intermediate field between F and L, K/F is normal, and that over K, f factors as $f(x) = g_1(x)\dots g_n(x)$, where each g_i is irreducible over K. Show that all the g_i's have the same degree.

Solution 8. Let g be one of the polynomials in $\{g_1, g_2, \dots, g_n\}$. Let α be a root of g and β the root of some g_i. By Lemma 0.1.18, there exists some $\sigma \in \mathrm{Gal}(L/F)$ such that $\sigma(\alpha) = \beta$. We define $\sigma(g)$ as the polynomial obtained by applying σ on the coefficients. By the normality of K/F, $\sigma(g) \in K[X]$ and $\sigma(g)$ is irreducible. It follows that $\sigma(g) = g_i$ (since they share a root) and deg g = deg g_i. Since, our choice of g and g_i was arbitrary, the result follows.

Problem 9. Let K/F be a finite Galois extension. For $\alpha \in K$, define the Norm and Trace of α by

(Norm) $$N_{K/F}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha)$$

(Trace) $$\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha)$$

(a) Show that $N_{K/F}(\alpha), \mathrm{Tr}_{K/F}(\alpha) \in F$ for all α in K.
(b) Show that $N_{K/F}$ is a homomorphism $K^\times \to F^\times$, and $\mathrm{Tr}_{K/F}$ is a homomorphism $(K,+) \to (F,+)$.
(c) Suppose that $\alpha = \sigma(\beta) - \beta$ for some $\sigma \in \mathrm{Gal}(K/F)$ and $\beta \in K$. Show that $\mathrm{Tr}_{K/F}(\alpha) = 0$.
(d) Suppose that $\alpha = \frac{\sigma(\beta)}{\beta}$ for some $\sigma \in \mathrm{Gal}(K/F)$ and $\beta \in K$. Show that $N_{K/F}(\alpha) = 1$.

Solution 9.

(a) $\mathrm{Gal}(K/F)$ fixes $N_{K/F}(\alpha)$ and $\mathrm{Tr}_{K/F}(\alpha)$. The result follows.
(b)

(Norm—Homomorphism)
$$N_{K/F}(\alpha\beta) = \prod_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha\beta) = \prod_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha) \times \prod_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\beta) = N_{K/F}(\alpha) \times N_{K/F}(\beta)$$

(Trace—Homomorphism)
$$\mathrm{Tr}_{K/F}(\alpha+\beta) = \sum_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha+\beta) = \sum_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\alpha) + \sum_{\sigma\in\mathrm{Gal}(K/F)} \sigma(\beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$$

(c) By part (b),
$$\mathrm{Tr}_{K/F}(\sigma(\beta)-\beta)=\mathrm{Tr}_{K/F}(\sigma(\beta))-\mathrm{Tr}_{K/F}(\beta)=0$$
since $\mathrm{Tr}_{K/F}(\sigma(\beta))=\mathrm{Tr}_{K/F}(\beta)$.

(d) By part (b),
$$N_{K/F}\left(\frac{\sigma(\beta)}{\beta}\right)=\frac{N_{K/F}\left(\sigma(\beta)\right)}{N_{K/F}\left(\beta\right)}=1$$
since $N_{K/F}(\sigma(\beta))=N_{K/F}(\beta)$.

Problem 10. Let $f(x)$ be a separable polynomial with coefficients in $\mathbb{Q}$, and let K denote its splitting field. Suppose that f has at least one (and hence at least two) nonreal roots. Show that $|\mathrm{Gal}(K/\mathbb{Q})|$ is even.

Solution 10. It suffices to prove the case where f is minimal (and hence separable). Consider the intermediate field L created by adjoining all real roots of f to $\mathbb{Q}$ and the polynomial $g\in L[X]$ formed by dividing out the real roots of f. By the *Complex Conjugate Root Theorem*, $\deg g$ is even. It follows that $[K:L]$ and, hence, $[K:\mathbb{Q}]$ are even.

Problem 11. Let $\alpha=\sqrt{6+\sqrt{11}}$ and $\beta=\sqrt{6-\sqrt{11}}$. Let $L=\mathbb{Q}(\alpha)$.

(a) What is the minimal polynomial of α?
(b) Show that $\beta\in L$.
(c) Show that $\{1,\alpha,\alpha^2,\alpha^3\}$ is a basis for L over $\mathbb{Q}$. Show that $\sqrt{11}\in L$ and express it in terms of this basis.
(d) Compute $\mathrm{Gal}(L/\mathbb{Q})$.
(e) Write α in the form $\sqrt{a}+\sqrt{b}$, for some $a,b\in\mathbb{Q}$.

Solution 11.

(a) $f(x)=(x^2-6)^2-11=x^4-12x^2+25$ has α as a root. By Lemma 0.1.11, f has no rational roots. Hence, if it did factor into the product of two lower degree polynomials, it would factor as the product of two quadratics (with integer coefficients by Gauss's Lemma). Suppose,
$$f(x)=(x^2+bx+5)(x^2+b'x+5).$$
Then,
$$\begin{aligned}b+b'&=0\\ bb'&=-22\end{aligned}$$
It follows that $(b')^2=22\implies b'\notin\mathbb{Z}$. Suppose
$$f(x)=(x^2+bx+1)(x^2+b'x+25).$$
Then,
$$\begin{aligned}b+b'&=0\\ 25b+b'&=0\\ bb'&=-38\end{aligned}$$
No solutions for this system of equations exists. Repeating similar arguments for the other two factorizations of f, it follows that f is irreducible.

(b) $f(\beta)=\left(\left(\sqrt{6-\sqrt{11}}\right)^2-6\right)^2-11=0$. If follows that the roots of f are
$$\alpha=\sqrt{6+\sqrt{11}}\qquad\alpha'=-\sqrt{6+\sqrt{11}}$$
$$\beta=\sqrt{6-\sqrt{11}}\qquad\beta'=-\sqrt{6-\sqrt{11}}$$

Call the splitting field of f F. Since $\alpha+\alpha'=0=\beta+\beta'$, we have that $\mathrm{Gal}(F/\mathbb{Q})\leq D_4$. Noting

$$\Delta=(\alpha-\alpha')^2(\alpha-\beta)^2(\alpha-\beta')^2(\alpha'-\beta)^2(\alpha'-\beta')^2(\beta-\beta')^2=774400=880^2,$$

$\mathrm{Gal}(F/\mathbb{Q})$ is strictly smaller than D_4. By part (a), we've bounded $|\mathrm{Gal}(F/\mathbb{Q})|$ below by 4. Since $[L:\mathbb{Q}]=4=[F:\mathbb{Q}]$ and $L\leq F$, $L=F$, and the desired result follows.

(c) The first follows directly from the minimality of f. For the second,

$$\alpha^2-6=\sqrt{11}.$$

(d) $\mathrm{Gal}(L/\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

(e)

$$\implies\sqrt{6+\sqrt{11}}=\sqrt{a}+\sqrt{b}$$
$$\implies 6+\sqrt{11}=a+b+\sqrt{4ab}$$

Using that $6=a+b$ and $11=4ab$ (and ignoring indistinct unordered pairs (a,b)), $a=11/2$ and $b=1/2$.

Problem 12. If K is the splitting field of some cubic polynomial $f(x)$ such that $\mathrm{Gal}(K/\mathbb{Q})\cong S_3$, then K contains a subfield F with $[F:\mathbb{Q}]=2$. What is F in terms of $f(x)$?

Solution 12. $F=\mathbb{Q}(\sqrt{\Delta})$.

Problem 13.

(a) Show that x^2+x+1 is irreducible over the field $\mathbb{F}_2$ with two elements, and let K denote its splitting field. Show that K is a field with four elements (we write it as $\mathbb{F}_4$). Compute $\mathrm{Gal}(K/\mathbb{F}_2)$.

(b) Let K denote the splitting field of x^3+x+1 over $\mathbb{F}_2$. How many elements does K have? Compute $\mathrm{Gal}(K/\mathbb{F}_2)$.

Solution 13.

(a) $0^2+0+1\equiv 1 \pmod 2$ and $1^2+1+1\equiv 1 \pmod 2$. The irreducibility of x^2+x+1 follows. Let α be a root of x^2+x+1. Then, the basis of $K/\mathbb{F}_2$ is $\{1,\alpha\}$. It follows that there are precisely $2^2=4$ elements in K. $\mathrm{Gal}(K/\mathbb{F}_2)=\{e,\sigma\}$ where $\sigma(\alpha)=\frac{1}{\alpha}$.

(b) By **Problem 18**, we have that $\mathrm{Gal}(K/\mathbb{F}_2)\cong A_3$ (S_3 is not cyclic). It follows that $|K|=2^3=8$.

Problem 14. Suppose that F is a (finite) field with p^n elements, for some prime p. Show that every element of F is a root of $x^{p^n}-x$.

Solution 14. $0^{p^n}-0=0$. By Lagrange's Theorem, for all x in the multiplicative group, $x^{p^n-1}-1=0$. The desired result follows.

Problem 15. Show that all finite fields with p^n elements are isomorphic. We call any such field $\mathbb{F}_{p^n}$.

Solution 15. Let F be a field of order p^n. We begin by showing there exists a field of order p within F by noting the existence of the field isomorphism $\sigma:\mathbb{F}_p\to F$ where $\sigma(\underbrace{1+1+\cdots+1}_{n\text{ times}})=\underbrace{1+1+\cdots+1}_{n\text{ times}}$. Now, consider a field K where $|K|=p^n$. Call the subfield of F and K respectively of order p F' and K'. There exists an isomorphism $\tau:F'\to K'$. Since both F and K are splitting fields of $x^{p^n}-x$, it follows that τ can be extended to an isomorphism $\rho:F\to K$ by Lemma 0.1.19.

Problem 16. Show that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m \mid n$.

Solution 16. Suppose $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$. Then,

$$p^n = p^{m \times [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]} \implies n = m \times [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}].$$

Now, suppose $n \mid m$. Then, $f(x) = x^{p^m} - x$ divides $g(x) = x^{p^n} - x$. It follows that the splitting field of g over $\mathbb{F}_p$ contains that of f over $\mathbb{F}_p$.

Problem 17. Show that the function $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\sigma(x) = x^p$ is an automorphism fixing $\mathbb{F}_p$. What is its order in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$? Compute $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Solution 17. We show σ fixes $\mathbb{F}_p$ by noting $0^p = 0$ and by applying Lagrange's Theorem on the multiplicative group. Let $x, y \in \mathbb{F}_{p^n}$

(Additive Homomorphism) $$(x+y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} y^i + y^P = x^p + y^p$$

(Multiplicative Homomorphism) $$(xy)^p = x^p y^p$$

It follows that σ is an automorphism (note the implicit use of Lemma 0.1.9). Since the multiplicative group of any finite field is cyclic, we can guarantee the existence of some α such that the order of α is $p^n - 1$ in the multiplicative group of $\mathbb{F}_{p^n}$. It follows that $|\sigma| = n$. Noting $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

Problem 18. Let $f(x) = x^3 + ax + b$ be an irreducible cubic polynomial, and let K be its splitting field. Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ unless $-4a^3 - 27b^2$ is a perfect square, in which case $\mathrm{Gal}(K/\mathbb{Q}) \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Solution 18. Call the roots of f α, β, γ. Noting $\gamma = -(\alpha + \beta)$ and by use of Vieta's formula,

$$\begin{aligned}
\Delta &= (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \\
&= (\alpha-\beta)^2(2\alpha+\beta)^2(2\beta+\alpha)^2 \\
&= 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 - 26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 \\
&= -4(\alpha\beta - \alpha(\alpha+\beta) - \beta(\alpha+\beta))^3 - 27(\alpha\beta(\alpha+\beta))^2 \\
&= -4a^3 - 27b^2
\end{aligned}$$

The desired result then follows.

Problem 19. Let F be a field and x transcendental over F . Let $\mathrm{GL}_2(F)$ denote the group of 2×2 matrices with entries in F with nonzero determinant, and let $Z(\mathrm{GL}_2(F))$ denote the center of $\mathrm{GL}_2(F)$. Let $\mathrm{PGL}_2(F)$ denote the quotient group $\mathrm{GL}_2(F)/Z(\mathrm{GL}_2(F))$. Show that $\mathrm{Aut}(F(x)/F) \cong \mathrm{PGL}_2(F)$.

Solution 19. For transcendental x, $F(x)$ consists of elements of the form $\frac{f(x)}{g(x)}$ where $f, g \in F[X]$. The elements of $\mathrm{Aut}(F(x)/F)$ are of the form $\sigma(f) = f \circ \phi$, where $\phi \in F(x)$. Now, noting that σ is bijective, there exsits $f \in F(x)$ such that $f \circ \phi = x$. By Lemma 0.1.20, it follows that ϕ is of the form

$$\phi(x) = \frac{ax+b}{cx+d}$$

with $ad \neq bc$. We prove all such ϕ extend to elements of $\mathrm{Aut}(F(x)/F)$ by noting, for $f, g \in F(x)$,

(Additive Homomorphism) $(f \circ \phi) + (g \circ \phi) = (f + g) \circ \phi$

(Multiplicative Homomorphism) $(f \circ \phi) \times (g \circ \phi) = (f \times g) \circ \phi$

Surjectivity follows from the existence of ϕ^{-1}. Now, define $\tau : \mathrm{Aut}(F(x)/F) \to \mathrm{PGL}_2(F)$ such that

$$\tau(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} Z(\mathrm{GL}_2(F))$$

where $\sigma(x) = \frac{ax+b}{cx+d}$. For some $\sigma' \in \mathrm{Aut}(F(x)/F)$, $\sigma'(x) = \frac{a'x+b'}{c'x+d'}$. Suppose $\sigma = \sigma'$ (I.e. $\frac{ax+b}{cx+d} = \frac{a'x+b'}{c'x+d'}$). It follows that

$$ac' = a'c \tag{16}$$

$$ad' + bc' = b'c + a'd \tag{17}$$

$$bd' = b'd \tag{18}$$

Noting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} da' - bc' & db' - bd' \\ ac' - ca' & ad' - cb' \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \in Z(\mathrm{GL}_2(F))$$

with $y = \frac{da'-bc'}{ad-bc} = \frac{ad'-cb'}{ad-bc}$, we conclude τ is well-defined. Seeing that

$$\sigma\sigma'(x) = \frac{a\frac{a'x+b'}{c'x+d'} + b}{c\frac{a'x+b'}{c'x+d'} + d} = \frac{(aa' + c'b)x + (ab' + bd')}{(ca' + dc')x + (cb' + dd')} \tag{19}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \tag{20}$$

we have that τ is a homomorphism. $\ker(\tau)$ is trivial since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathrm{GL}_2(F)) \implies a = d,\ b = c = 0 \implies \frac{ax + b}{cx + d} = x,$$

and $\mathrm{im}(\tau) = \mathrm{PGL}_2(F)$ since

$$\tau(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \sigma(x) = \frac{ax + b}{cx + d}.$$

Problem 20. Let a and b be integers, and let $f(x) = x^4 + ax^2 + b$. Assume that $f(x)$ is irreducible over $\mathbb{Q}$, and let K be the splitting field for $f(x)$ over $\mathbb{Q}$. Show that

- If b is a perfect square, then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- If $b(a^2 - 4b)$ is a perfect square, then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.
- Otherwise, $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.

This result is known as *Kaplansky's Theorem*.

Solution 20. Call the roots of f $\{x, y, -x, -y\}$. Since $x - x = 0 = y - y$, $\mathrm{Gal}(K/\mathbb{Q}) \leq D_4$.

$$\begin{aligned} \Delta &= ((x-y)(x-(-x))(x-(-y))(y-(-x))(y-(-y))(-x-(-y)))^2 \\ &= \left((4xy)(x-y)^2(x+y)^2\right)^2 \\ &= 16x^2y^2(x^4 + y^4 - 2x^2y^2)^2 \\ &= 16b(4b - a^2)^2 \end{aligned}$$

Since, by Vieta's formula,

$$a = -(x^2 + y^2) \tag{21}$$

$$b = x^2y^2 \tag{22}$$

(i) $\sqrt{\Delta} \in \mathbb{Q} \iff \sqrt{b} \in \mathbb{Q}$. Noting the only subgroup of D_4 in A_4 is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the desired results follows.

(ii) Since f is irreducible, $\sqrt{b} \notin \mathbb{Q}$ since $\sqrt{b} \in \mathbb{Q}$ implies $\sqrt{a^2-4b} \in \mathbb{Q}$, and, hence, f factors as

$$f(x) = \left(x^2 - \frac{-a+\sqrt{a^2-4b}}{2}\right)\left(x^2 - \frac{-a-\sqrt{a^2-4b}}{2}\right).$$

Since $\sqrt{b(a^2-4b)} = xy(x^2-y^2) \in \mathbb{Q}$, we have that the map $\tau = (x,-x)$ doesn't fix $\sqrt{b(a^2-4b)}$. Then, $\mathrm{Gal}(K/\mathbb{Q})$ isn't $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (or D_4) — the only remaining option being $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

(iii) From (i) and (ii) (and their converses), $\mathrm{Gal}(K/\mathbb{Q})$ isn't $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. The only other possibility is D_4.

Problem 21. Let $p_1, p_2, \ldots, p_n$ be distinct prime numbers. Let $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Show that $[K:\mathbb{Q}] = 2^n$.

Solution 21. Consider the intermediate field $F_k = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$. We claim that for any subset $S \subseteq \{p_{k+1}, \ldots, p_n\}$, $\prod_{x\in S} \sqrt{x} \notin F_k$.

($k=1$) Let $S = \{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$. Suppose $\sqrt{p_{i_1}p_{i_2}\ldots p_{i_m}} = a + b\sqrt{p_1}$. Then,

$$0 = (a^2 + b^2 p_1 - p_{i_1}p_{i_2}\ldots p_{i_m}) + 2ab\sqrt{p_1}.$$

If $a = 0$, $b = \sqrt{\frac{p_{i_1}p_{i_2}\cdots p_{i_m}}{p_1}}$, which contradicts that b is rational. If $b = 0$, $a = \sqrt{p_{i_1}p_{i_2}\ldots p_{i_m}}$, which contradicts that a is rational. The desired result follows.

($k > 1$) Suppose the statement holds for $k-1$, and let $S = \{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$. Then, note $F_k = F_{k-1}(\sqrt{p_k})$. Suppose $\sqrt{p_{i_1}p_{i_2}\ldots p_{i_m}} = a + b\sqrt{p_k}$ with $(a, b \in F_{k-1})$. Then,

$$0 = (a^2 + b^2 p_k - p_{i_1}p_{i_2}\ldots p_{i_m}) + 2ab\sqrt{p_k}.$$

If $a = 0$, we have that $bp_k = \sqrt{p_{i_1}p_{i_2}\ldots p_{i_m}p_k}$, which contradicts the inductive hypothesis, and, if $b = 0$, $a = \sqrt{p_{i_1}p_{i_2}\ldots p_{i_m}}$, contradicting the inductive hypothesis.

It follows that $\sqrt{p_{k+1}} \notin F_k$, and, hence, $[K:\mathbb{Q}] = 2^n$.

Problem 22. Let $K = F(x_1, \ldots, x_n)$ denote the field of rational functions in n variables over a field F. For $1 \le i \le n$, let s_i denote the ith *elementary symmetric polynomial* in $x_1, \ldots, x_n$, given by

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
s_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2\ldots x_n
\end{aligned}$$

(a) Show that if $f(x_1, \ldots, x_n)$ is any rational function in $x_1, \ldots, x_n$ that is symmetric in $x_1, \ldots, x_n$ (i.e. $f(x_1, x_2, \ldots, x_n) = f(x_2, x_1, \ldots, x_n)$, and similarly for permuting the variables in any way), then f can be expressed in terms of $s_1, \ldots, s_n$.

(b) Show that the automorphism group $\mathrm{Aut}(K/F)$ has a subgroup H isomorphic to the symmetric group S_n, given by permuting the indices of the x_i's.

(c) Show that $K^H = F(s_1, \ldots, s_n)$.

Solution 22.

(a) Phrased differently, the desired results is

Given a symmetric rational function f, $f \in F(s_1, \ldots, s_n)$.

It suffices to prove the result for polynomials in $x_1, \ldots, x_n$. For monomial $f(x) = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$, define deg $f = (e_1, e_2, \ldots, e_n)$. We extend this to polynomials by use of a lexicographic ordering. That is, for $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ in N^n, $(x_1, x_2, \ldots, x_n) > (y_1, y_2, \ldots, y_n)$ if, for the first i such that $x_i \neq y_i$, $x_i > y_i$. Then, for an arbitrary polynomial f, deg f is the degree of the largest monomial in f. Naturally, call this monomial the leading term of f (denoted lead f). Now, we proceed by induction on the degrees. Noting $F \subset F(s_1, \ldots, s_n)$, the constant polynomial belongs in $F(s_1, \ldots, s_n)$. Then, suppose f is a symmetric polynomial with lead $f = a x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$. Since

$$\deg (f \times g) = (\deg f) + (\deg g),$$

we have that lead $a s_1^{e_1 - e_2} s_2^{e_2 - e_3} \ldots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n} =$ lead f, and, hence, by the inductive hypothesis,

$$(f - a s_1^{e_1 - e_2} s_2^{e_2 - e_3} \ldots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n}) \in F(s_1, \ldots, s_n) \implies f \in F(s_1, \ldots, s_n).$$

(b) Define $\phi : S_n \to \mathrm{Aut}(K/F)$ as $\phi(\sigma) = \tau_\sigma$ where

$$\tau_\sigma(f(x_1, x_2, \ldots, x_n)) = f(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)).$$

Noting the follow,

(Additive Field Homomorphism)

$$\tau_\sigma(f(x_1, x_2, \ldots, x_n) + g(x_1, x_2, \ldots, x_n)) = \tau_\sigma(f(x_1, x_2, \ldots, x_n)) + \tau_\sigma(g(x_1, x_2, \ldots, x_n))$$

(Multiplicative Field Homomorphism)

$$\tau_\sigma(f(x_1, x_2, \ldots, x_n) \times g(x_1, x_2, \ldots, x_n)) = \tau_\sigma(f(x_1, x_2, \ldots, x_n)) \times \tau_\sigma(g(x_1, x_2, \ldots, x_n))$$

(Surjectivity) $\tau_\sigma\big(f(\sigma^{-1}(x_1), \sigma^{-1}(x_2), \ldots, \sigma^{-1}(x_n))\big) = f(x_1, x_2, \ldots, x_n)$

(Group Homomorphism) $\tau_{\sigma_2}(\tau_{\sigma_1}(f(x_1, x_2, \ldots, x_n))) = \tau_{\sigma_2 \sigma_1}(f(x_1, x_2, \ldots, x_n))$

we have that ϕ is a well-defined, homomorphism. The injectivity of ϕ follows from noting that if $\sigma \neq e$, there exists distinct i, j such that $\sigma(i) = j$. Hence, $\tau_\sigma \neq e$ since τ_σ doesn't fix x_i, and $\ker(\phi)$ is trivial.

(c) By part (a), $K^H = F(s_1, \ldots, s_n)$.

CHAPTER 2.4

Insolvability of the Quintic

Problem 1. Find the roots of $x^3 - 5x^2 + 5$.

Solution 1. Let $x = y + \frac{5}{3}$. Applying this substitution, we get

$$\begin{aligned}
&= x^3 - 5x^2 + 5 \\
&= \left(y + \frac{5}{3}\right)^3 - 5\left(y + \frac{5}{3}\right)^2 + 5 \\
&= y^3 + 5y^2 + 25y + \frac{125}{27} - 5y^2 - \frac{25}{9} - \frac{50}{3}y + 5 \\
&= y^3 + \frac{25}{3}y + \frac{185}{27}
\end{aligned}$$

Setting $y = \alpha + \beta$ where $3\alpha\beta = -\frac{25}{3}$,

$$\begin{aligned}
&= (\alpha+\beta)^3 + \frac{25}{3}(\alpha+\beta) + \frac{185}{27} \\
&= \alpha^3 + 3\beta^3 + 3\alpha\beta(\alpha+\beta) + \frac{25}{3}(\alpha+\beta) + \frac{185}{3} \\
&= \alpha^3 + \beta^3 + \frac{185}{27} \\
&= \frac{\alpha^6 + \frac{185}{27}\alpha^3 - \left(\frac{25}{9}\right)^3}{\alpha^6}
\end{aligned}$$

Setting $x^3 - 5x^2 + 5 = 0$,

$$\alpha^6 + \frac{185}{27}\alpha^3 - \left(\frac{25}{9}\right)^3 = 0 \implies \alpha^3 = \frac{5\left(\sqrt{2688001} - 962\right)}{1404}.$$

It follows that

$$\alpha \in \left\{ \sqrt[3]{\frac{5\left(\sqrt{2688001} - 962\right)}{1404}}, \sqrt[3]{\frac{5\left(\sqrt{2688001} - 962\right)}{1404}}\zeta_3, \sqrt[3]{\frac{5\left(\sqrt{2688001} - 962\right)}{1404}}\zeta_3^2 \right\}$$

and $x = a - \frac{25}{9a} + \frac{5}{3}$.

Problem 2. Show that if K/F is a Galois extension and L/F is any extension, then KL/L is Galois, and $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$.

Solution 2. By **Problem 7** of the previous chapter, KL/L is Galois. Define our homomorphism $\tau : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/K \cap L)$ by taking restrictions. That is, $\tau(\sigma)$ is the restriction of σ onto $K \to K$. Since σ fixes L, $\tau(\sigma)$ fixes $L \cap K$, and the automorphism properties of σ transfer to $\tau(\sigma)$. τ is injective since $\ker(\tau)$ is trivial. $\mathrm{im}(\tau) = \mathrm{Gal}(K/E)$ where $K/E/K \cap L$ is some intermediate field. Since E is fixed by the restrictions of $\mathrm{Gal}(KL/L)$, we have $E \subseteq L$ and, hence, $E = K \cap L$. We conclude τ is an isomorphism.

Problem 3. Find, with proof, an irreducible sixth degree polynomial whose Galois group is not solvable.

Solution 3. Consider $f(x) = x^6 - 10x^2 + 2x + 6$. By Eisenstein's criterion with $p = 2$, f is irreducible. Denote the roots of f α_1, α_2, α_3, α_4, α_5, and α_6.

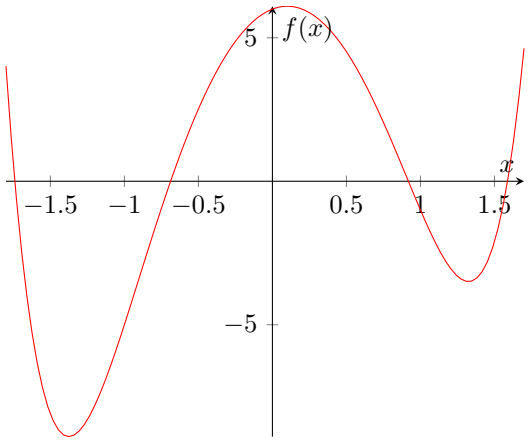


FIGURE 1. $f(x) = x^6 - 10x^2 + 2x + 6$ has 4 real roots.

Call the splitting field of f L and let $H_i = \mathrm{Gal}(L/\mathbb{Q}(\alpha_i))$. We prove $f(x)/(x - \alpha_i)$ is irreducible over $\mathbb{Q}(\alpha_i)$. Notice that this is equivalent to showing $5 \mid \mathrm{Gal}(L/\mathbb{Q})$. Consider the polynomial $\overline{f} = x^6 + 2x + 1$, constructed by reducing the coefficients of f modulo 5. Call the splitting field of $\overline{f}$ over $\mathbb{F}_5$ K. As $\overline{f} \equiv (x-4)(x^5 + 4x^4 + x^3 + 4x^2 + x + 1) \pmod 5$, K is the splitting field of $g(x) = x^5 + 4x^4 + x^3 + 4x^2 + x + 1$. We hope to prove g is irreducible. By observation, g has no roots in $\mathbb{F}_5$. Hence, we factor g as

$$g(x) = (x^3 + ax^2 + bx + 1)(x^2 + cx + 1) = x^5 + (c+a)x^4 + (1 + ac + b)x^3 + (a + bc + 1)x^2 + (b + c)x + 1.$$

It follows that

$$\begin{aligned} c + a = 4 &\implies a = 4 - c \\ ac + b = 1 & \\ a + bc = 3 & \\ b + c = 1 &\implies b = 1 - c \end{aligned}$$

Solving for c, we find that $(4-c)c + (1-c) = 0 \implies c^2 - 3c - 1 = 0$ and $(4-c) + c(1-c) = 3 \implies c^2 = 1$. It follows that no solutions exist for the above system of equations, and, hence, g is irreducible. By Lemma 0.1.23, 5 divides $|\mathrm{Gal}(K/\mathbb{F}_p)|$ and $|\mathrm{Gal}(L/\mathbb{Q})|$. Now, we show $\mathrm{Gal}(L/\mathbb{Q})$ acts 2-transitively on the roots. Consider the subsets of the set of roots $\{\alpha_j, \alpha_k\}$ and $\{\alpha_{j'}, \alpha_{k'}\}$. As $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the roots (Lemma 0.1.18), we choose $f \in \mathrm{Gal}(L/\mathbb{Q})$ such that $f(\alpha_j) = \alpha_{j'}$. Similarly, as $H_{j'}$ acts transitively on $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\} \setminus \{\alpha_{j'}\}$ and fixes $\alpha_{j'}$, we choose $g \in H_{j'}$ such that $(g \circ f)(\alpha_k) = \alpha_{k'}$. Now, since complex conjugation is a 2-cycle in our Galois group, $\mathrm{Gal}(L/\mathbb{Q})$ contains a transposition and is the full symmetric group of degree 6 (Lemma 0.1.22).

Problem 4. Let $\zeta_n = e^{2\pi i/n}$. Compute the degrees $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})]$ and $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}]$.

Solution 4.

($n > 2$) Note ζ_n is a root of $x^2 - (\zeta_n + \zeta_n^{-1})x + 1$. Since $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \leq \mathbb{R}$ (and $\mathbb{Q}(\zeta_n) \not\leq \mathbb{R}$),

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$$

$$[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\phi(n)}{2}$$

$(n = 1, 2)$ $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 1$ and $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = 1$

Problem 5. Find the minimal polynomials of $\zeta_7 + \zeta_7^{-1}$ and $\zeta_7 + \zeta_7^2 + \zeta_7^4$.

Solution 5. Notice $\zeta_7 + \zeta_7^{-1} = 2\cos\left(\frac{2\pi}{7}\right)$. Using a result from **Problem 2** of Chapter 2, our minimal polynomial is $f(x) = 8(x/2)^3 + 4(x/2)^2 - 4(x/2) - 1 = x^3 + x^2 - 2x - 1$. Since

$$\begin{aligned}
&= \left(\zeta_7 + \zeta_7^2 + \zeta_7^4\right)^2 + \zeta_7 + \zeta_7^2 + \zeta_7^4 \\
&= \zeta + 2\zeta^2 + 2\zeta^3 + 2\zeta^4 + 2\zeta^5 + 2\zeta^6 + \zeta^8 \\
&= 2(1 + \zeta + 2\zeta^2 + 2\zeta^3 + 2\zeta^4 + 2\zeta^5 + 2\zeta^6) - 2 \\
&= 2\Phi_7(\zeta_7) - 2 = -2
\end{aligned}$$

the minimal polynomial of $\zeta_7 + \zeta_7^2 + \zeta_7^4$ is $g(x) = x^2 + x + 2$.

Problem 6. Let p be a prime and a an integer. Define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a perfect square modulo } p, \\ -1 & a \text{ is a nonsquare modulo } p, \\ 0 & a \equiv 0 \pmod{p}. \end{cases}$$

(a) Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(b) Let

$$g(a, p) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an}.$$

Show that $g(a, p) = \left(\frac{a}{p}\right) g(1, p)$. Conclude that for any a with $\gcd(a, p) = 1$, $g(a, p)^2 = g(1, p)^2$.

(c) If ζ_p is a primitive root of unity, compute

$$\sum_{a=0}^{p-1} \zeta_p^{an}$$

in terms of n.

(d) Compute $g(0, p)$.

(e) Show that

$$g(1, p)^2 = \begin{cases} p & p \equiv 1 \pmod{4}, \\ -p & p \equiv 3 \pmod{4} \end{cases}$$

by evaluating

$$\sum_{a=0}^{p-1} g(a, p) g(-a, p)$$

in two ways.

Solution 6.

(a)
- **The product of two quadratic residues is a quadratic residue:** $x^2 y^2 \equiv (xy)^2 \pmod{p}$.
- **The product of a quadratic residue and a non-residue is a non-residue:** $x^2 y \equiv z^2 \mod p \implies y \equiv \left(\frac{z}{x}\right)^2$

- **The product of two quadratic non-residues is a residue:** Let a be a non-residue. Note that $ax \equiv ay \pmod{p} \iff x \equiv y \pmod{p}$. Then, since the map $f : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ where $f(x) = ax$ is injective and sends all quadratic residues to non-residues (and by point 1 of Lemma 0.1.21), it follows that all non-residues are sent to residues.

The result follows.

(b) Let the kth summand in $g(a,p)$ be $\left(\frac{k}{p}\right)\zeta_p^{ak} = \left(\frac{k}{p}\right)\zeta_p^j$ where $ak \equiv j$ is a residue modulo p. Then,

$$\left(\frac{aj}{p}\right)\zeta_p^j = \left(\frac{k^{-1}j^2}{p}\right)\zeta_p^j = \left(\frac{k}{p}\right)\zeta_p^j,$$

and, hence, the desired result follows.

(c)
$$\sum_{a=0}^{p-1} \zeta_p^{an} = \begin{cases} p & a \equiv 0 \pmod{p}, \\ 0 & a \not\equiv 0 \pmod{p}. \end{cases}$$

(d) $g(0,p) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0$, by point 1 of Lemma 0.1.21.

(e) For integral $m \in [0, p-1]$, denote c_{ma} as the coefficient of ζ_p^{ma} in $g(a,p)g(-a,p)$. By expanding out $g(a,p)g(-a,p)$, we find that for non-zero a,

$$c_{ma} = \begin{cases} p-1 & m \equiv 0 \pmod{p}, \\ \left(\frac{1(1-m)}{p}\right) + \left(\frac{2(2-m)}{p}\right) + \cdots + \left(\frac{(p-1)(p-1-m)}{p}\right) & m \not\equiv 0 \pmod{p}. \end{cases}$$

By point 3 of Lemma 0.1.21, for all non-zero m, $c_{ma} = -1$. Hence,

$$g(a,p)g(-a,p) = p - 1 + -(\Phi_p(\zeta_p) - 1) = p.$$

Then,

$$\sum_{a=0}^{p-1} g(a,p)g(-a,p) = (g(0,p))^2 + \sum_{a=1}^{p-1} p = p(p-1).$$

Alternatively, we can write $\sum_{a=0}^{p-1} g(a,p)g(-a,p)$ as

$$\sum_{a=0}^{p-1} g(a,p)g(-a,p) = g(1,p)^2 \sum_{a=0}^{p-1} \left(\frac{-a^2}{p}\right) = g(1,p)^2 \sum_{a=1}^{p-1} \left(\frac{-1}{p}\right).$$

By point 2 of Lemma 0.1.21, we have that $g(1,p)^2 = p$ for $p \equiv 1 \pmod{4}$ and $-p$ otherwise.

Problem 7. In this problem, we prove the famous quadratic reciprocity theorem. For an odd prime p, let

$$p^* = \begin{cases} p & p \equiv 1 \pmod{4}, \\ -p & p \equiv 3 \pmod{4}. \end{cases}$$

Let us write g for $g(1,p)$. Let q be an odd prime different from p.

(a) Show that $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod{q}$.

(b) Show that $g^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. Thus, $g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q}$.

(c) Show, using the binomial theorem, that $g^q \equiv g(q,p) \pmod{q}$.

(d) Show that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.

(e) Evaluate $\left(\frac{-1}{q}\right)$.

(f) Show that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Solution 7.

(a) Notice that

$$\left(a^{\frac{q-1}{2}}-1\right)\left(a^{\frac{q-1}{2}}+1\right)\equiv a^{q-1}-1\equiv 0 \pmod{p}.$$

Since there are precisely $\frac{q-1}{2}$ quadratic residues (point 1, Lemma 0.1.21) and every quadratic residue a satisfies $a^{\frac{q-1}{2}}-1\equiv 0 \pmod{q}$, the result follows.

(b) By part (e) of **Problem 6**,

$$\left(\frac{p^*}{q}\right)\equiv (p^*)^{\frac{q-1}{2}}\equiv \left(g^2\right)^{\frac{q-1}{2}}\equiv g^{q-1} \pmod{q}.$$

(c) By the Binomial Theorem (Lemma 0.1.9), $(a+b)^q\equiv a^q+b^q \pmod{q}$ since $q \mid \binom{n}{i}$ for $i\notin\{0,n\}$. By induction, we can extend this to the case with multiple summands. Hence,

$$g^q\equiv\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta_p^{qn}\equiv g(q,p) \pmod{q}.$$

(d) By part (c) and part (b),

$$\left(\frac{p^*}{q}\right)\equiv g^{q-1}\equiv\frac{\left(\frac{q}{p}\right)g}{g}\equiv\left(\frac{q}{p}\right) \pmod{q}.$$

Since q is an odd prime and the legendre symbol only outputs $1,-1$, and 0, the result follows.

(e) See point 2 of Lemma 0.1.21.

(f) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\left(\frac{pp^*}{q}\right)$. If $p\equiv 1 \pmod{4}$ (I.e. $p=4k+1$),

$$\left(\frac{pp^*}{q}\right)=\left(\frac{p^2}{q}\right)=1=(-1)^{2k\times\frac{q-1}{2}}=(-1)^{\frac{(p-1)(q-1)}{4}}.$$

If $p\equiv 3 \pmod{4}$ (I.e. $p=4k+3$),

$$\left(\frac{pp^*}{q}\right)=\left(\frac{-1}{q}\right)=(-1)^{\frac{q-1}{2}}=(-1)^{\frac{q-1}{2}\times(2k+1)}=(-1)^{\frac{(p-1)(q-1)}{4}}.$$

Problem 8. If $n>2$, then $\phi(n)=|(\mathbb{Z}/n\mathbb{Z})^\times|$ is even. This means that $\mathbb{Q}(\zeta_n)$ has a subfield K (possibly more than one) with $[K:\mathbb{Q}]=2$. Thus, K can be expressed as $\mathbb{Q}(\sqrt{d})$ for some d. Find a suitable d, in terms of n. Can you find all such d?

Solution 8. For any odd prime p dividing n, let $d=p^*$. If n is a power of 2, let $d=-1$. Now, suppose $n=p_1^{e_1}\times p_2^{e_2}\times\cdots\times p_m^{e_m}$ where the p_i's are odd primes. Then,

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times&\cong(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times\times(\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/p_m^{e_m}\mathbb{Z})^\times\\&\cong\mathbb{Z}/(p_1^{e_1}-p_1^{e_1-1})\mathbb{Z}\times\mathbb{Z}/(p_2^{e_2}-p_2^{e_2-1})\mathbb{Z}\times\cdots\times\mathbb{Z}/(p_m^{e_m}-p_m^{e_m-1})\mathbb{Z}\end{aligned}$$

Noting that the number of index 2 subgroups is the same as the number of order 2 subgroups, we count the number of order two elements to note there are 2^m-1 quadratic subfields. Let $S=\{p_1^*,p_2^*,\ldots,p_m^*\}$. Then,

$$d\in\left\{x\in\mathbb{C}|x=\prod_{a\in S}a \text{ for any non-empty subset } S \text{ of } P\right\}.$$

For the special case where n is even, let $n=2^k\times p_2^{e_2}\times\cdots\times p_m^{e_m}$. Then, our set S changes to

(k=1) $S = \{p_2^*, \ldots, p_m^*\}$

(k=2) $S = \{-1, p_2^*, \ldots, p_m^*\}$

(k>2) $S = \{2, -2, p_2^*, \ldots, p_m^*\}$

Problem 9. Suppose $[F(\alpha) : F]$ is odd. Show that $F(\alpha) = F(\alpha^2)$.

Solution 9. Since $f(x) = x^2 - \alpha^2 \in F(\alpha^2)[X]$ and $f(\alpha) = 0$, $[F(\alpha) : F(\alpha^2)] \in \{1, 2\}$. Since $[F(\alpha) : F]$ is odd, $F(\alpha) = F(\alpha^2)$.

Problem 10. Suppose that D is a non-square, positive integer that can be written as a sum of two squares. Show that there is an extension $L/\mathbb{Q}(\sqrt{D})$ such that L is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Hint: Consider $\mathbb{Q}\left(\sqrt{D + a\sqrt{D}}\right)$, where $D = a^2 + b^2$.

Solution 10. Let L be the splitting field of $f(x) = (x^2 - D)^2 - a^2 D = x^4 - 2Dx^2 + (D^2 - a^2 D)$. To prove the irreducibility of f, it suffices to show $\sqrt{D + a\sqrt{D}} \notin \mathbb{Q}(\sqrt{D})$. Suppose there exists rational x and y such that $\sqrt{D + a\sqrt{D}} = x + y\sqrt{D} \implies D + a\sqrt{D} = x^2 + y^2 D + 2xy\sqrt{D}$. Setting $D = x^2 + y^2 D$ and $a = 2xy \implies y = \frac{a}{2x}$,

$$D = x^2 + \frac{a^2 D}{4x^2} \implies 4x^4 - 4Dx^2 + a^2 D = 0.$$

For the polynomial $g(z) = 4z^2 - 4Dz + a^2 D$,

$$\Delta_g = 16D^2 - 16a^2 D = 16(a^4 + b^4 + 2a^2 b^2 - a^4 - a^2 b^2) = 16b^2(b^2 + a^2) = 16b^2 D$$

is not a perfect square in $\mathbb{Q}$. It follows that no such x and y exist. Applying Kaplansky's Theorem, $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ since $(D^2 - a^2 D)(4D^2 - 4(D^2 - a^2 D)) = 4a^2 D^2 b^2$ is a perfect square in $\mathbb{Q}$.

Problem 11. Show that if D is not a sum of two squares, then there is no such L as in the previous problem. Conclude that there is no $\mathbb{Z}/4\mathbb{Z}$ extension containing $\mathbb{Q}(\sqrt{3})$.

Solution 11. We hope to show the quadratic sub-field of any $\mathbb{Z}/4\mathbb{Z}$ extension $L/\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{D})$ for non-square, integer D, where D is the sum of squares in $\mathbb{Q}$. Consider the tower $L/\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Since $L = \mathbb{Q}(\sqrt{a + b\sqrt{D}})$ for some $a, b \in \mathbb{Q}$, we have that L is the splitting field of $f(x) = x^4 - 2ax^2 + (a^2 - b^2 D)$. As f is irreducible, we apply Kaplansky's Theorem to note

$$\sqrt{(a^2 - b^2 D)(4a^2 - 4(a^2 - b^2 D))} = \sqrt{(a^2 - b^2 D)4b^2 D} \in \mathbb{Q} \implies (a^2 - b^2 D)D = c^2$$

for some $c \in \mathbb{Q}$. It follows $D = \left(\frac{c}{a}\right)^2 + \left(\frac{bD}{a}\right)^2$. Now, for integer n, p, q, r, $n = \left(\frac{p}{r}\right)^2 + \left(\frac{q}{r}\right)^2 \implies r^2 n = p^2 + q^2$. By the *Sum of Two Square Theorem*, the prime decomposition of n contains no primes congruent to 3 modulo 4 raised to an odd power, and, hence, n is the sum of squares in $\mathbb{Z}$. The desired then follows.

Problem 12. Show that if p is prime and G is a transitive, solvable subgroup of S_p, then G is contained in a Frobenius group, which is a group of order $p(p-1)$. (One interpretation of a Frobenius group in S_p is the normalizer of a Sylow p-subgroup).

Solution 12. We first show that every non-trivial normal subgroup H of G is transitive. Call the orbits induced by the action of H $O_1, O_2, \ldots, O_m$. Let $\tau \in G$ and $i, j \in O_q$. I.e. there exists $\sigma \in H$ such that $\sigma(i) = j$.

(1) If $\tau(i) \in O_{q'}$, $\tau(j) \in Q_{q'}$ since $(\tau\sigma\tau^{-1})(\tau(i)) = \tau(j)$.

(2) If $\exists \alpha \in H$ such that $\alpha(\tau(i)) = k$, then $k = \tau\left((\tau^{-1}\alpha\tau)(i)\right)$.

As G is transitive, $|O_1| = |O_2| = \cdots = |O_m| \in \{1, p\}$. As H is non-trivial, H is transitive. To show the Sylow p-subgroup P of G is normal in G, we proceed by induction on the length of our solvable series. If G is abelian, the result follows immediately. Suppose $\{e\} \trianglelefteq \cdots \trianglelefteq H \trianglelefteq G$. Since H is transitive and solvable, the inductive hypothesis guarantees $P \trianglelefteq H$. For $g \in G$, $gPg^{-1} \leq gHg^{-1} = H$. By the Sylow Theorems, normality in H is equivalent to uniqueness in H, and, hence, $gPg^{-1} = P$.

Problem 13. Suppose that F is a field of characteristic not dividing n, and suppose further that F contains all the nth roots of unity. Fix $a \in F^\times$, and let $K = F(\sqrt[n]{a})$. Show that K/F is a Galois extension, and $\mathrm{Gal}(K/F)$ is cyclic of order dividing n.

Solution 13. As the roots of $x^n - a$ are of the form $\sqrt[n]{a}$, $\sqrt[n]{a}\zeta_n$, $\sqrt[n]{a}\zeta_n^2, \ldots, \sqrt[n]{a}\zeta_n^{n-1}$, K/F is both normal and separable. Define the map $f : \mathrm{Gal}(K/F) \to \mathbb{Z}/n\mathbb{Z}$ such that $f(\sigma_m) = m$ if $\sigma_m(a) = \sqrt[n]{a}\zeta_n^m$. As f is a homomorphism, $\mathrm{Gal}(K/F)$ is cyclic with order dividing n.

Problem 14. Suppose K/F is a finite Galois extension, and $\mathrm{Gal}(K/F) = \{\sigma_1, \ldots, \sigma_n\}$. Show that $\sigma_1, \ldots, \sigma_n$ are linearly independent, in the sense that if $c_1, \ldots, c_n \in F$ satisfy

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0$$

for all $x \in K$, then $c_1 = \cdots = c_n = 0$. This result is known as *linear independence of characters*.

Solution 14. We proceed by induction. Suppose $c_1\sigma_1(x) + c_2\sigma_2(x) = 0$ for all $x \in K$. Setting $x = 1$, $c_1 = -c_2$. Choosing y such that $\sigma_1(y) \neq \sigma_2(y)$, $c_1(\sigma_1(y) - \sigma_2(y)) = 0 \implies c_1 = c_2 = 0$. Now, suppose $c_1\sigma_1(x) + \cdots + c_m\sigma_m(x) = 0$. Choosing y such that $\sigma_1(y) \neq \sigma_m(y)$,

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_m\sigma_m(y)\sigma_m(x) = 0 \tag{23}$$

$$c_1\sigma_m(y)\sigma_1(x) + \cdots + c_m\sigma_m(y)\sigma_m(x) = 0 \tag{24}$$

Subtracting (14) from (13),

$$c_1\sigma_1(x)(\sigma_1(y) - \sigma_m(y)) + \cdots + c_{m-1}\sigma_{m-1}(x)(\sigma_{m-1}(y) - \sigma_m(y)) = 0.$$

By the inductive hypothesis, $c_1 = 0$. Repeating this argument for the other c_i's, the result follows.

Problem 15. Let F be as in **Problem 13**, and let K/F be a Galois extension with $\mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$. Let σ be a generator of $\mathrm{Gal}(K/F)$. For $\alpha \in K$ and an nth root of unity ζ, define the *Lagrange Resolvent* as

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

(a) Show that $(\alpha, \zeta)^n \in F$.
(b) Show that if ζ is a primitive n^{th} root of unity, then there is some $\alpha_0 \in K$ such that $(\alpha_0, \zeta) \neq 0$.
(c) Show that (α_0, ζ) does not lie in any proper subfield of K.
(d) Conclude that if $a = (\alpha_0, \zeta)$, then $K = F(\sqrt[n]{a})$.

Solution 15.

(a) Noting $\sigma((\alpha, \zeta)) = \zeta(\alpha, \zeta)$, $\sigma\left((\alpha, \zeta)^n\right) = \zeta^n(\alpha, \zeta)^n = (\alpha, \zeta)^n$.
(b) By The Linear Independence of Characters, such α_0 must exist.
(c/d) Noting $\sigma^m((\alpha_0, \zeta)) = \zeta^m(\alpha_0, \zeta)$, we have that (α_0, ζ) isn't fixed by any non-identity elements of $\mathrm{Gal}(K/F)$. The desired results follow.

Part 3

Ring Theory & Algebraic Geometry

CHAPTER 3.1

Rings and Ideals

Problem 1. Prove Proposition 2.6: For a ring R,

(1) The additive and multiplicative identities 0 and 1 are unique.
(2) Additive inverses are unique.
(3) $(-1) \times (-1) = 1$.
(4) For any $a \in R$, $a \times 0 = 0$.
(5) For any $a \in R$, $(-1) \times a = -a$.

Solution 1.

(1) The uniqueness of 0 follows from noting R is a group under addition. For the uniqness of 1, consider the two additive identities 1 and $1'$. As $1 \times r = r = 1' \times r$ for all $r \in R$, set $r = 1$ and the result follows.
(2) Once again, this follows from noting R is a group under addition.
(3) By (4) and (5), $-1 \times -1 + -1 \times 1 = -1(-1 + 1) = -1 \times 0 = 0 \implies -1 \times -1 = 1$.
(4) $b = a \times (0 + 0) = a \times 0 + a \times 0 = b + b \implies b = 0$.
(5) $1 \times a + (-1) \times a = a(1 \times -1) = 0 \implies -1 \times a = -a$.

Problem 2. Let R be a ring. Show that if $a \in R$ is a unit, then it is not a zero divisor.

Solution 2. $ab = 0 \implies b = a^{-1} \times 0 = 0$.

Problem 3. Show that any subring of a field is an integral domain.

Solution 3. For such a subring, every element has an inverse in the field. By **Problem 2**, the result follows.

Problem 4. Show that if $I \subseteq R$ is an ideal and I contains a unit, then $I = R$.

Solution 4. We have the first inclusion for free. For unit a in I, $a^{-1}a = 1 \in I \implies R \subseteq I$.

Problem 5. Show that if R is an integral domain and $a, b \in R$ are such that $(a) = (b)$, then there is a unit $u \in R$ so that $b = au$.

Solution 5. If $ab = 0$, then $a = b = 0$. In which case, we choose $u = 1$. If $ab \neq 0$, there exists $u, u' \in R$ such that $au = b$ and $bu' = a$. Then, $(ab)(uu') = ab \implies uu' = 1$. I.e. u is a unit.

Problem 6. In which rings R is the ideal (0) a prime ideal?

Solution 6. Integral domains.

Problem 7. Show that commutativity of addition follows automatically from the other ring axioms, even without assuming commutativity of multiplication.

Solution 7. By use of associativity and distributivity,

$$\begin{aligned}(a+b)-(b+a) &= a+b-b-a \\ &= a+(b-b)-a \\ &= a-a=0\end{aligned}$$

Problem 8. Show that a nontrivial finite integral domain (i.e. one with only finitely many elements, but more than just one) is a field.

Solution 8. Let R be our ring. For arbitrary $a \in R$ ($a \neq 0$), define $f : R \to R$ such that $f(x) = ax$. f is injective and, hence, surjective. Then, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$. R then satisfies the field axioms.

Problem 9. Show that if I and J are ideals of a ring R and $I + J = R$, then $I \cap J = IJ$. Find a counterexample when $I + J \neq R$.

Solution 9. We note $IJ \subset I \cap J$. As $I + J = R$, we can write an arbitrary element of $I \cap J$ as $a + b$ and $1 = a' + b'$ for $a, a' \in I$ and $b, b' \in J$. Since $a + b \in I \cap J$, $a \in J$ and $b \in I$. Hence,

$$a + b = (a' + b')a + (a' + b')b = aa' + ab' + ba' + bb' \in IJ.$$

For our counterexample, let $R = \mathbb{Z}$, $I = (2)$, and $J = (4)$. $I + J = I \neq R$ and $IJ = (8) \neq (4) = I \cap J$.

Problem 10. Give an example of a ring R and ideals I and J such that $\{ij : i \in I, j \in J\}$ is not closed under addition. This explains why the definition of ideal multiplication is what it is.

Solution 10. Let $R = \mathbb{Z}$, $I = (2, x)$, $J = (3, x)$. Then,

$$(x + 4)(x + 6) + 2 \times 3 = x^2 + 10x + 30 \notin \{ij : i \in I, j \in J\}.$$

Problem 11. Show that $\mathbb{R}[x]$ is a PID. Show that $\mathbb{Z}[x]$ is not a PID by showing that $(2, x)$ is not a principal ideal.

Solution 11. Let I be an ideal in $\mathbb{R}[x]$. $I = \{0\} \implies I = (0)$. For $I \neq \{0\}$, choose the smallest non-zero degree polynomial f. For $g \in I$,

$$g(x) = q(x)f(x) + r(x) \implies r(x) = g(x) - q(x)f(x) \in I \implies r(x) = 0.$$

Hence, $I = (f)$. Suppose $(2, x) = (g)$ for some $g \in \mathbb{Z}[x]$. If $\deg g = 0$, $2 \mid g$ since the elements of I have even constant terms. Then, $x \notin I$. If $\deg g > 0$, $2 \notin I$. (Alternatively, the result follows directly from Lemma 0.1.24).

Problem 12. We now know that $\mathbb{Z}$ and $\mathbb{R}[x]$ are PIDs. Express $(12, 18) \subseteq \mathbb{Z}$ and $(x^2+x, x^2+2x+1) \subseteq \mathbb{R}[x]$ as principal ideals, generated by single elements.

Solution 12.

- As $6 \mid 12, 18$ and $18 - 12 = 6$, $(12, 18) = (6)$.

- As $x+1 \mid x^2+x, x^2+2x+1$ and $x+1 = (x^2+2x+1)-(x^2+x)$, $(x^2+2x+1, x^2+x) = (x+1)$.

Problem 13. Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial, and let $p \in \mathbb{Z}$ be a prime. When is $(p, f(x))$ a prime ideal of $\mathbb{Z}[x]$? Explain why $(2, x^2+1)$ is not a prime ideal.

Solution 13. Denote the reduction of f modulo p $\overline{f}$. Applying Lemma 0.1.25,

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(\overline{f}(x))}$$

and, hence, $(p, f(x))$ is prime iff $\overline{f}(x)$ is prime in $\mathbb{Z}/p\mathbb{Z}[x]$ (since both quotients have to be integral domains). Noting that prime elements are irreducible and $x^2+1 \equiv (x-1)(x+1) \pmod 2$, $(2, x^2+1)$ is not a prime ideal.

Problem 14. Let $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ be an irreducible polynomial. Show that $(f) \subseteq k[x_1, \ldots, x_n]$ is a prime ideal. Find a prime ideal of $k[x_1, \ldots, x_n]$ that is not of this form.

Solution 14. It suffices to show f is prime. By Lemma 0.1.26 and induction, $k[x_1, \ldots, x_n]$ is a UFD, and, hence, f is prime. By Lemma 0.1.24, the second part isn't possible for $n = 1$. For $n > 2$, call $R = k[x_1, \ldots, x_n]$ and, hence, $R[x_n] = k[x_1, \ldots, x_n]$. For prime $p \in R$ (for example, $p = x_1$), consider

$$I = \{q(x_n) \in R[x_n] |\ q(0) \in (p)\}.$$

The primality of I follows from that of p. Now, assuming $I = (f)$, then $\deg f = 0$ and $f = p$ since $p \in I$. Then, $x_n - p = p(ax_n + b) = pax_n + pb \implies 1 = ap$, contradicting the primality of p.

Problem 15.

(a) Find examples of rings with exactly one maximal ideal. Fields have this property, but can you find others? (Such rings are called *local rings*).
(b) Show that if R is a local ring with maximal ideal $\mathfrak{m}$, then $R^\times = R/\mathfrak{m}$.

Solution 15.

(a) By **Problem 18** of the next chapter, $\mathbb{Z}/(4)$ has precisely one non-zero ideal.
(b) As $\mathfrak{m} \neq R$, $R/\mathfrak{m} \subset R^\times$. Now, consider $x \in R/\mathfrak{m}$. If x is a non-unit, $(x) + \mathfrak{m} = R$ and there exists $y \in R$ and $m \in \mathfrak{m}$ such that $xy + m = 1$. As $(m) = (1 - xy), (x) \in \mathfrak{m}$, $1 = 1 - xy + xy \in \mathfrak{m} = R$.

Problem 16. Compare the ideals of $\mathbb{Z}$ and the ideals of $\mathbb{Z}[1/2]$. What happens with prime and maximal ideals?

Solution 16. The prime and maximal ideals of $\mathbb{Z}$ are of the form (p) for prime $p \in \mathbb{Z}$. For $\mathbb{Z}[1/2]$, we begin by noting

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^b} |\ a \text{ is odd},\ b \in \mathbb{Z}\right\}.$$

Consider an ideal $I \subset \mathbb{Z}[1/2]$. Noting that $I \cap \mathbb{Z} = (x)$ $(x \in \mathbb{Z})$ is an ideal of $\mathbb{Z}$ and, for integral a, $a/2^b \in I \iff a \in I$, we have that $I = (x)$. It suffices to determine the prime integers of $\mathbb{Z}[1/2]$. Let p be an odd prime. Then, for odd integers a, b, c,

$$\frac{c}{2^{m'}}p = \frac{ab}{2^m} \implies cp = ab \implies p \mid a \text{ or } p \mid b.$$

Noting that 2 and -2 are units, we conclude the prime ideals in $\mathbb{Z}[1/2]$ are of the form (p) for odd prime $p \in \mathbb{Z}$. We note that these prime ideals are all maximal since, for $a/2^b \notin (p)$, $a \in (a/2^b) + (p)$ and, hence, by

Bézout's Lemma $(\gcd(a,p)=1)$, $1 \in (a/2^b)+(p) \implies (a/2^b)+(p) = \mathbb{Z}[1/2]$.

Problem 17. Show that the following conditions on a ring R are equivalent:

(1) Every ideal of R is finitely generated.
(2) The ideals of R satisfy the *ascending chain condition*: if $I_1 \subseteq I_2 \subseteq I_3 \subset \dots$ is an ascending chain of ideals of R, then there is some $N > 0$ so that, whenever $m, n > N$, then $I_m = I_n$. Such a chain is said to stabilize.
(3) If S is any nonempty collection of ideals of R, then S has a maximal element, i.e. there is some $I \in S$ such that there is no $J \in S$ properly containing I.

When these conditions are satisfied, R is said to be a *noetherian* ring.

Solution 17.

(1) $\implies$ (2) Suppose there exists a chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. By (1), $\bigcup_{n=1}^{\infty} I_n$ is finitely generated. Noting that these generators can be found in finitely many I_i's, it follows that the chain stabilizes
(2) $\implies$ (1) We prove the contrapositive. Consider an infinitely generated ideal $(x_1, x_2, \dots)$ and the chain $(x_1), (x_1, x_2), \cdots$.
(2) $\implies$ (3) The existence of a collection S of ideals without a maximal element breaks the the ascending chain condition.
(3) $\implies$ (2) Consider the ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ and the collection S of I_i's. As there exists a maximal element I_m, $I_m = I_n$ for all $n \geq m$.

Problem 18. Prove the Hilbert basis theorem, which says that if R is a noetherian ring, then so is the polynomial ring $R[x]$, and hence by induction $R[x_1, \dots, x_n]$.

Solution 18. Consider an arbitrary ideal $I \subset R[x]$. We hope to show I is finitely generated. Consider the chain of ideals of R $\mathfrak{m}_0 \subset \mathfrak{m}_1 \subset \mathfrak{m}_2 \subset \cdots$ where

$$\mathfrak{m}_i = \{r \in R | \ \exists f \in I \text{ such that } \deg f = i \text{ and lead } f = r\}.$$

As R is notherian, we say the chain terminates at $\mathfrak{m}_n$. Call the generators of $\mathfrak{m}_i$ $\{m_1, \dots, m_k\}$. Then, let $S_i = \{f_1, f_2, \dots, f_k\}$ where $f_j \in I$, lead $f_j = m_j$, and deg $f_j = i$. We prove that $S = \bigcup_{i=0}^{n} S_i$ generates I by induction on the degrees of the elements of I. For degree 0 polynomials, the result is apparent since the generators of $\mathfrak{m}_0 = S_0$. For $f \in I$ with deg $f > 0$, we construct g using S such that lead g = lead f and deg g = deg f. By the inductive hypothesis, $f - g$ can be generated by the S, and, hence, the result follows.

Problem 19. Show that the ring $R[x_1, x_2, x_3, \dots]$ of polynomials in infinitely many variables is not noetherian.

Solution 19. Consider the infinite chain

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots.$$

CHAPTER 3.2

Homomorphism and Quotients

Problem 1. Which of the following rings are isomorphic to each other?

(1) $\mathbb{Z}/60\mathbb{Z}$
(2) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
(3) $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
(4) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$
(5) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

Solution 1. By the *Chinese Remainder Theorem*,

- $(\mathbb{Z}/60\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$
- $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z})$

Note $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}) \ncong \mathbb{Z}/60\mathbb{Z}$ because $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z})$ has no order 4 element.

Problem 2. Do there exist integers satisfying the following congruences? If so, find the smallest such positive integer.

(a) $4 \pmod 5$, $3 \pmod 6$, $8 \pmod{11}$
(b) $4 \pmod 6$, $5 \pmod 8$, $9 \pmod{13}$
(c) $3 \pmod 6$, $1 \pmod 8$, $5 \pmod{11}$

Solution 2.

(a) By application of the *Chinese Remainder Theorem*,

$$x \equiv (8 \cdot 7 \cdot 5 \cdot 6) + (5 \cdot 11 \cdot 3) + (6 \cdot 11 \cdot 4) \equiv 129 \pmod{330}.$$

(b) No solutions exist as the first two congruence are contradictory: if $x \equiv 4 \pmod 6$, x is even, but, if $x \equiv 5 \pmod 8$, x is odd.

(c) Note $x \equiv 3 \pmod 6$ iff $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 3$ by CRT. Since $x \equiv 1 \pmod 2$ is already implied by $x \equiv 1 \pmod 8$, our problem is reduced to solving the congruences

$$0 \pmod 3,\ 1 \pmod 8,\ 5 \pmod{11}.$$

By the *Chinese Remainder Theorem*,

$$x \equiv (8 \cdot 11 \cdot 3) + (5 \cdot 3 \cdot 8 \cdot 6) + (11 \cdot 3) \equiv 225 \pmod{264}.$$

Problem 3. Is $\mathbb{R}[x]/(x^2+1)$ an integral domain? A field? What about $\mathbb{C}[x]/(x^2+1)$? Why do these behave differently?

Solution 3. By Lemma 0.1.27, $\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}(i) = \mathbb{C}$, which is both a field and an integral domain. By the *Chinese Remainder Theorem* and Lemma 0.1.27,

$$\frac{\mathbb{C}[x]}{(x^2+1)} \cong \frac{\mathbb{C}[x]}{(x+i)} \times \frac{\mathbb{C}[x]}{(x-i)} \cong \mathbb{C} \times \mathbb{C}.$$

As $(0,1) \times (1,0) = 0$ and $(0,1)$ has no inverse, $\mathbb{C} \times \mathbb{C}$ is neither a field nor an integral domain. Note that the principal reason these quotients are different is because x^2+1 is irreducible in $\mathbb{R}$ but not in $\mathbb{C}$.

Problem 4. Show that if $f : R \to S$ is a homomorphism, then $f(-r) = -f(r)$ for all $r \in R$.

Solution 4. $f(-r) + f(r) = f(r - r) = f(0) = 0 \implies -f(r) = f(-r)$.

Problem 5. Show that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

Solution 5. Assuming an isomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Q}[x]$ exists, we note $\phi(f(x)) = f(\phi(x))$ as, for all $n \in \mathbb{Z}$, $\phi(n) = \phi(1 + 1 + \cdots + 1) = n$ or $\phi(n) = \phi(-1 - 1 - 1 \cdots - 1) = n$. If $\deg \phi(x) = 0$, $f \notin \text{im}(\phi)$ if $\deg f > 0$, and, if $\deg \phi(x) > 0$, non-integer, rational $q \notin \text{im}(\phi)$.

Problem 6. Let R be a ring. Describe all homomorphisms $f : \mathbb{Z} \times \mathbb{Z} \to R$.

Solution 6. Note that $\mathbb{Z} \times \mathbb{Z}$ is generated by $(0, 1)$ and $(1, 0)$. It follows f is uniquely defined by where it sends $(0, 1)$ and $(1, 0)$. Noting that

$$1 = f((1, 1)) = f((0, 1) + (1, 0)) = f((0, 1)) + f((0, 1)) \tag{25}$$

$$0 = f((0, 0)) = f((0, 1) \times (1, 0)) = f((0, 1)) \times f((0, 1)), \tag{26}$$

we require f to send $(0, 1)$ and $(1, 0)$ such that the above equalities are satisfied.

Problem 7. Let R be a ring. Describe all the homomorphisms $f : \mathbb{Z}[x] \to R$. What about $f : \mathbb{Z}[x_1, \ldots, x_n] \to R$? Under what conditions are they injective? Surjective?

Solution 7. Noting that $\forall n \in \mathbb{Z}$, $f(n) = f(\pm 1 \pm 1 \pm \cdots \pm 1) = n$, the homomorphisms $f : Z[x] \to R$ are of the form $f(g(x)) = g(f(x))$ where $f(x)$ can be any element of R. For $f : \mathbb{Z}[x_1, \ldots, x_n] \to R$, $f(g(x_1, x_2, \ldots, x_n) = g(f(x_1), f(x_2), \ldots, f(x_n))$ where $f(x_i)$ can be any element of R. For f to be injective, $f(x_i)$ must be transcendental over $f(\mathbb{Z})[f(x_1), \ldots, f(x_{i-1}), f(x_{i+1}), \ldots, f(x_n)]$. For f to be surjective, $S = \{f(x_1), f(x_2), \ldots, f(x_n)\}$ must generate R.

Problem 8. Find a ring homomorphism $f : R \to S$ and an ideal I of R such that $f(I)$ is not an ideal of S.

Solution 8. Consider the inclusion map $f : \mathbb{Z} \to \mathbb{Q}$. $f((n))$ for non-zero n isn't an ideal.

Problem 9. An isomorphism from a ring to itself is called an automorphism. Describe all the automorphisms of the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[x]$, and $Z \times Z$.

Solution 9.

- Consider an isomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$. As $\phi(1) = 1$ and $\phi(-1) = -1$, ϕ is the identity map.
- Consider an isomorphism $\phi : \mathbb{Q} \to \mathbb{Q}$. Noting that $\phi(x)\phi\left(\frac{1}{x}\right) = \phi(1) = 1 \implies \phi\left(\frac{1}{x}\right) = \frac{1}{\phi(x)}$ and ϕ fixes $\mathbb{Z}$,

$$\phi\left(\frac{p}{q}\right) = \frac{\phi(p)}{\phi(q)} = \frac{p}{q}.$$

  I.e. ϕ is the identity map.
- Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ be an isomorphism. As ϕ fixes $\mathbb{Z}$, $\phi(g(x)) = g(\phi(x))$. Hence, $\phi(x)$ uniquely determines ϕ. Noting that $\deg g(\phi(x)) = \deg g(x) \times \deg \phi(x)$, $\deg \phi(x) = 1$ by the surjectivity of ϕ. In particular, $\phi(x)$ must be invertible as there exists f such that $f(\phi(x)) = x$. I.e. $\phi(x) = x + b$

for $b \in \mathbb{Z}$. We note that all these maps are isomorphisms because

(Additive Homomorphism) $\phi(f(x) \times g(x)) = f(\phi(x)) \times g(\phi(x)) = \phi(f(x)) \times \phi(g(x))$

(Multiplicative Homomorphism) $\phi(f(x) + g(x)) = f(\phi(x)) + g(\phi(x)) = \phi(f(x)) + \phi(g(x))$

(Multiplicative Identity is Fixed) $\phi(1) = 1 \circ \phi(x) = 1$

(Injectivity) $\phi(f(x)) = \phi(g(x)) \implies f(\phi(x)) = g(\phi(x)) \implies f(x) = g(x)$

(Surjectivity) $\phi(f(x)) = g(x) \implies f(x) = (g \circ \phi^{-1})(x)$

- Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be an isomorphism. Note $(0,1)$ and $(1,0)$ generate $\mathbb{Z} \times \mathbb{Z}$. It follows ϕ is uniqely determined by where it sends $(0,1)$ and $(1,0)$. By Equations 25 and 26 of **Problem 6**, $\phi((0,1)) = (a,b) \implies \phi((1,0)) = (1-a, 1-b)$ and $a(a-1) = 0 \implies a = 0, 1$ and $b(b-1) = 0 \implies b = 0, 1$. Using the injectivity of ϕ, ϕ is either the identity or $\phi((0,1)) = (1,0)$ and $\phi((1,0)) = (0,1)$.

Problem 10. Show that $\mathbb{C}[x]/(p(x))$, where p is a degree-n polynomial in $\mathbb{C}[x]$, is isomorphic to $\mathbb{C} \times \cdots \times \mathbb{C}$ (n times) if and only if p has no repeated roots. (You may assume the fundamental theorem of algebra.)

Solution 10. Let $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. By the *Chinese Remainder Theorem* and Lemma 0.1.27,

$$\begin{aligned} \frac{\mathbb{C}[x]}{p(x)} &\cong \frac{\mathbb{C}[x]}{(x-\alpha_1)} \times \frac{\mathbb{C}[x]}{(x-\alpha_2)} \times \cdots \times \frac{\mathbb{C}[x]}{(x-\alpha_n)} \\ &\cong \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{n \text{ times}} \end{aligned}$$

since $(x - \alpha_i) - (x - \alpha_j) = \alpha_j - \alpha_i \in (x - \alpha_i) + (x - \alpha_j)$ is a unit.

Problem 11. Consider the ring $\mathbb{Z}[i]$, where $i = \sqrt{-1}$. For an integer n, let (n) denote the ideal of $\mathbb{Z}[i]$ consisting of all multiples of n in $\mathbb{Z}[i]$. For each integer n, describe the structure of the quotient ring $\mathbb{Z}[i]/(n)$. When is $\mathbb{Z}[i]/(n)$ an integral domain?

Solution 11. In the hope of classifying the prime ideals of $\mathbb{Z}[i]$ of the form (n) ($n \in \mathbb{Z}$), we restrict our attention to prime $n > 0$. Suppose $n \mid (a + bi)(c + di) = (ac - bd) + (ad + bc)i$. I.e.

$$ac - bd \equiv 0 \pmod{n} \tag{27}$$

$$ad + bc \equiv 0 \pmod{n} \tag{28}$$

Suppose $n \nmid (c + di)$. If $n \mid c$,

$$ad \equiv bd \equiv 0 \pmod{n} \implies a \equiv b \equiv 0 \pmod{n},$$

and, similarly, if $n \mid d$,

$$ac \equiv bc \equiv 0 \pmod{n} \implies a \equiv b \equiv 0 \pmod{n}.$$

If $n \nmid c, d$, $b \equiv acd^{-1} \pmod{n}$. Substituting into Equation 28,

$$ad + ac^2d^{-1} \equiv 0 \pmod{n} \implies a(d^2 + c^2) \equiv 0 \pmod{n}.$$

Noting that $d^2 + c^2 \equiv 0 \pmod{n} \implies (dc^{-1})^2 \equiv -1 \pmod{n}$, we use Lemma 0.1.21 to conclude n is prime if $n \equiv 3 \pmod{4}$. For $n \equiv 1 \pmod{4}$, write $n = a^2 + b^2 = (a + bi)(a - bi)$ to note n isn't prime.

Problem 12. For each prime p, explain how to construct a field with p^2 elements.

Solution 12. Choose an irreducible quadratic f over $\mathbb{F}_p$. For odd p, consider $f(x) = x^2 - a$ for non-quadratic residue a, and, for $p = 2$, consider $f(x) = x^2 + x + 1$. By Lemma 0.1.27, we note

$$\frac{\mathbb{F}[x]}{(f)} \cong \mathbb{F}_{p^2}.$$

Problem 13. Let $\mathbb{R}[[x]]$ be the set of formal power series with coefficients in $\mathbb{R}$, i.e. the set whose elements are "infinite polynomials" $\sum_{n=0}^{\infty} a_n x^n$ with $a_n \in \mathbb{R}$. Show that $\mathbb{R}[[x]]$ is a ring and describe all its ideals.

Solution 13. We define addition and multiplication in the normal sense:

$$\sum_{n=0}^{\infty} a_n x_n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$
$$\sum_{n=0}^{\infty} a_n x_n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n.$$

Verifying the ring axioms, we note $\mathbb{R}[[x]]$ is a ring:

- The addition and multiplication of power series is both associative and commutative by the associativity and commutativity of $+$ and $\times$ in $\mathbb{R}$.
- The additive identity is the 0 polynomial and the multiplicative identity is the 1 polynomial.
- The additive inverse of $f(x)$ is $-1 \times f(x)$.
- Multiplication is distributive over addition:

$$= \left(\sum_{n=0}^{\infty} c_n x_n \right) \left(\sum_{n=0}^{\infty} a_n x_n + \sum_{n=0}^{\infty} b_n x^n \right)$$
$$= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} c_i (a_{n-i} + b_{n-i}) \right) x^n$$
$$= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} c_i a_{n-i} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} c_i b_{n-i} \right) x^n.$$

We begin by classifying the units of $\mathbb{R}[[x]]$. Consider $f(x) = \sum_{n=0}^{\infty} a_n x^n$. If $a_0 \neq 0$, $f(x)g(x)$ has a zero constant term. For $a_n \neq 0$, we inductively construct the inverse $g(x) = \sum_{n=0}^{\infty} b_n x^n$ as

$$b_0 = \frac{1}{a_0} \tag{29}$$

$$b_k = -\frac{1}{a_0} \sum_{n=1}^{k} a_0 b_{k-n}. \tag{30}$$

With this, we proceed to show $R[[x]]$ is a PID. In particular, for an ideal I, $I = (x^k)$ where

$$k = \min \left\{ i \in \mathbb{N} | \, \exists \sum_{n=0}^{\infty} a_n x^n \in I \text{ where } a_i \neq 0 \right\}.$$

Note that $x^k \in I$ because there exists $f(x) \in I$ for which $f(x) = a_k x^k + a_{k+1} x^{k+1} + \cdots = x^k \left(a_k + a_{k+1} x + \cdots \right) \implies x^k = f(x) \left(a_k + a_{k+1} x + \cdots \right)^{-1} \in I$. Since $x^k \nmid p(x) \in I$ contradicts the minimality of k, the desired result follows.

Problem 14. Prove Proposition 1.6: A homomorphism $f : R \to S$ is an isomorphism if and only if there is a homomorphism $g : S \to R$ such that $g \circ f : R \to R$ and $f \circ g : S \to S$ are the identity isomorphisms.

Solution 14. The homomorphism property of f plays no role in our proof. Considering f as a map, it suffices to show f is bijective iff f has an inverse g. Assuming f is bijective, we construct $g : R \to S$ such that $g(x) = y$ if $f(y) = x$. g is well-defined since f is injective. Letting $f(x) = y$ and $g(x) = y'$,

(from the definition of g) $(g \circ f)(x) = g(f(x)) = g(y) = g(x)$

(contradiction) $(f \circ g)(x) = f(g(x)) = f(y') \neq x \implies g(x) \neq y'$

For the reverse direction, suppose f is invertible. I.e. there exists a map g such that $g \circ f$ and $f \circ g$ are identity maps. f is surjective because $f(x) = k \implies x = g(k)$, and f is injective because

$$f(x) = f(x') \implies g(f(x)) = g(f(x')) \implies x = x'.$$

Problem 15. Prove Proposition 3.1: Addition and multiplication of cosets is well-defined. That is, if $a + I = a' + I$ and $b + I = b' + I$, then $(a + b) + I = (a' + b') + I$, and similarly $(ab) + I = (a'b') + I$.

Solution 15. We note that $a' = a + i$ for $i \in I$ and $b = b' + j$ for $j \in I$. Then, by closure under addition and the absorption property,

(Addition Is Well-defined) $(a + b) - (a' + b') = (a - a') + (b - b') \in I$

(Multiplication Is Well-defined) $ab - a'b' = ab - (a + i)(b + j) = -aj - ib - ij \in I.$

Problem 16. Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ are ideals of a ring R. Show that $\bigcup_{n=1}^{\infty} I_n$ is also an ideal of R. Show that it is prime if all the I_n's are prime. Show the analogous statements for descending chains and intersections: if $J_1 \supseteq J_2 \supseteq J_3 \supseteq \cdots$ are ideals of R, then $\bigcap_{n=1}^{\infty} J_n$ is an ideal of R, and it is prime if all the J_n's are.

Solution 16.

- Consider $a, b \in \bigcup_{n=1}^{\infty} I_n$ (i.e. $\exists m$ such that $a, b \in I_m$) and $r \in R$. As $ra \in I_m$ and $a + b \in I_m$, $\bigcup_{n=1}^{\infty} I_n$ is an ideal. Assuming the I_n's are prime, $xy \in \bigcup_{n=1}^{\infty} I_n \implies \exists m$ such that $xy \in I_m$. By the primality of I_m, $x \in I_m \implies x \in \bigcup_{n=1}^{\infty} I_n$ or $y \in I_m \implies y \in \bigcup_{n=1}^{\infty} I_n$. I.e. $\bigcup_{n=1}^{\infty} I_n$ is prime.
- Similarly, consider $a, b \in \bigcap_{n=1}^{\infty} J_n$ (i.e. $a, b \in J_n$ for all $n \in \mathbb{N}$) and $r \in R$. Noting that $a, b \in J_n \implies a + b \in J_n$ and $a \in J_n \implies ra \in J_n$ for all $n \in \mathbb{N}$, $\bigcap_{n=1}^{\infty} J_n$ is an ideal. Assuming the primality of the J_n's, suppose $ab \in \bigcap_{n=1}^{\infty} J_n$ with $a \notin \bigcap_{n=1}^{\infty} J_n$ and $b \notin \bigcap_{n=1}^{\infty} J_n$. I.e. there exists J_p and J_q such that $a \notin J_p$ and $b \notin J_q$. WLOG, suppose $p > q$ (if $p = q$, we contradict the primaility of J_p). Then, $J_p \subseteq J_q$, and, by the primality of J_p, $b \in J_p \implies b \in J_q$. (contradiction!)

Problem 17. Prove the following other isomorphism theorems:

(a) If I and J are ideals of R, then $(I + J)/J \cong I/(I \cap J)$.
(b) If I and J are ideals of R with $I \subseteq J$, then J/I is an ideal of R/I, and $(R/I)/(J/I) \cong R/J$.

Solution 17.

(a) Consider the homomorphism $\phi : I \to (I + J)/J$ where $\phi(x) = x + J$. As the ideals of $(I + J)/J$ are of the form $i + j + J = i + J$ for $i \in I$ and $j \in J$, ϕ is surjective. Further noting $\ker(\phi) = I \cap J$, the desired result follows from the *First Isomorphism Theorem.*
(b) As J is closed under addition, J/I is closed under addition. As J is an ideal, for $a \in R$ and $j \in J$, $(a + I)(j + I) = aj + I \in J/I$. Now, consider the homomorphism $\phi : R/I \to R/J$ where $\phi(x + I) = x + J$. Noting that ϕ is surjective and $\phi(x + I) = J \iff x \in J$ (i.e. $\ker(\phi) = J/I$), the desired result follows from the *First Isomorphism Theorem.*

Problem 18. Let R be a ring and I an ideal of R. Find a bijection between ideals of R/I and ideals of R containing I.

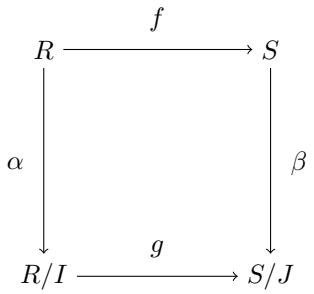
Solution 18. Call S the set of ideals of R containing I and S' the set of ideals of R/I. Define $f : S \to S'$ by $f(K) = K/I$ (note that K/I must be ideal of R/I from **Problem 17** part (b)).

- Suppose $K/I = K'/I$. Then, for all $k' \in K'$, there exists $k \in K$ such that $k + I = k' + I \implies k' - k \in I \subseteq K$. Hence, $k' \in K$ and $K' \subseteq K$. By symmetry, $K \subseteq K'$ and $K = K'$. In other words, f is injective.
- For an ideal J of R/I, construct $J' = \bigcup_{x \in J} x$. As $I \in J$, $I \subseteq J'$, and J' is an ideal because, for $a, b \in J'$ and $r \in R$,

$$a + I, b + I \in J \implies a + b + I \in J \implies a + b \in J'$$
$$(r + I)(a + I) = ar + I \in J' \implies ar \in J'.$$

  Since $J = J'/I$, f is surjective.

Problem 19. Let R and S be rings, and let I and J be ideals of R and S, respectively. From a homomorphism $f : R \to S$, we obtain a homomorphism $R \to S/J$ by composing f with the projection map $S \to S/J$. Show that f gives us a ring homomorphism $g : R/I \to S/J$ if and only if $f(I) \subseteq J$. When this happens, show that the following diagram commutes, meaning that either way of following arrows from R to S/J gives the same answer:



Solution 19. Define $g(x + I) = f(x) + I$. For $a, b \in R$,

(Additive Homomorphism) $$g(a + b + I) = f(a + b) + J = f(a) + J + f(b) + J = g(a) + g(b)$$

(Multiplicative Homomorphism) $$g(ab + I) = f(ab) + J = (f(a) + J)(f(b) + J) = g(a) \times g(b)$$
$$g(1 + I) = f(1) + J = 1 + J.$$

For $i \in I$, $g(I) = g(i + I) = f(i) + J = J \implies f(i) \in J$. I.e. $f(I) \subseteq f(J)$. If $F(I) \not\subseteq J$, $\exists i \in I$ such that $f(i + I) = i + J \neq J$. So, f is potentially not well-defined and doesn't fix 0. For $r \in R$,

$$(g \circ \alpha)(r) = g(r + I) = f(r) + I = (\beta \circ f)(r).$$

Problem 20. Let R and S be two rings. Describe the ideals of $R \times S$ in terms of the ideals of R and S and determine which ones are prime and maximal. What are their quotients?

Solution 20. Let K be an ideal in R. We note $K = I \times J$ where I and J are

$$I = \{i \in R | \ \exists j \in S \text{ such that } (i, j) \in K\}$$
$$J = \{j \in S | \ \exists i \in R \text{ such that } (i, j) \in K\}.$$

For $r \in R$ and $i, i' \in I$, our definitions guarantee there exists $j, j' \in R$ such that $(i, j), (i', j') \in K$. Then,

(Closure Under Addition) $$(i, j) + (i', j') = (i + i', j + j') \in K \implies i + i' \in I$$

(Absorption) $$r(i, j) = (ri, rj) \in K \implies ri \in I$$

Applying a similar argument for J, we conclude I and J are ideals. Since $I \times J$ is an ideal of $R \times S$ when $I \subseteq R, J \subseteq S$ are ideals (applying a similar argument once again), we know the form of ideals in $R \times S$. Naturally, the prime ideals are $\mathfrak{p} \times \mathfrak{q}$ for prime $\mathfrak{p} \subseteq R, \mathfrak{q} \subseteq S$. For prime $K \subseteq R \times S$, write $K = \mathfrak{p} \times \mathfrak{q}$. If $ab \in \mathfrak{p}$, there exists $c \in S$ such that $(ab, c) = (a, 1)(b, c) \in K \implies (a, 1) \in K$ or $(b, c) \in K$. I.e. $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Applying a similar argument for $\mathfrak{q}$, the result follows. However, all ideals of the form $\mathfrak{p} \times \mathfrak{q}$ are not prime. Let $R = S = \mathbb{Z}$, $\mathfrak{p} = (2)$, and $\mathfrak{q} = (3)$. Note $(2, 5)(5, 3) \in (2) \times (3)$ but neither multiplicands lie in $(2) \times (3)$. For maximal ideals, if $\mathfrak{m} \subset R$, $\mathfrak{n} \subset S$ are maximal in R and S, the maximal ideals are of the form $R \times \mathfrak{n}$ or $\mathfrak{m} \times S$. We note if $K = \mathfrak{m} \times \mathfrak{n}$ where $\mathfrak{m} \neq R$ and $\mathfrak{n} \neq S$, $K \subset \mathfrak{m} \times S \neq R \times S$. I.e. K is not maximal. For the opposite direction, we consider $\mathfrak{m} \times S$ where $\mathfrak{m}$ is maximal. If $\mathfrak{m} \times S \subseteq I \times J$, $J = S$, and the maximality of $\mathfrak{m}$ guarantees $I = R$. For the quotients, we note that (for ideals $I \subseteq R$, $J \subseteq S$),

$$\frac{R \times S}{I \times J} \cong \frac{R}{I} \times \frac{S}{J}.$$

Consider the homomorphism $\phi : R \times S \to R/I \times S/J$ where $\phi((a, b)) = (a + I, b + J)$. As ϕ is surjective and $\ker(\phi) = \{(a, b) \in R \times S |\ a \in I \text{ and } b \in J\} = I \times J$, the desired result follows from the *First Isomorphism Theorem*.

Problem 21. An ideal I of R is called primary if, whenever $a, b \in R$ are such that $ab \in I$, then either $a \in I$ or $b^n \in I$ for some positive integer n.

(a) Describe all the primary ideals in $\mathbb{Z}$ and $\mathbb{R}[x]$.
(b) Show that an ideal $I \subset R$ is primary if and only if, for every zero divisor a of the quotient ring R/I, $a^n = 0$ for some positive integer n.

Solution 21.

(a) Using part (b), we note $(m) \subseteq \mathbb{Z}$ is primary if and only if for all $a \in \mathbb{Z}/m\mathbb{Z}$ with $\gcd(a, m) \neq 1$, there exists $n \in \mathbb{N}$ for which $a^n \equiv 0 \pmod{m}$. If $m = p^k$ for prime p, $a^k \equiv 0 \pmod{m}$. If m is divisible by two primes p, q, $p^n \not\equiv 0 \pmod{m}$ for all $n \in \mathbb{N}$. To conclude, (m) is primary iff $m = p^k$ for prime p and integer k. Similarly, for $\mathbb{R}[x]$, $(f) \subseteq \mathbb{R}[x]$ is primary iff $f(x) = (g(x))^k$ for irreducible g. Suppose $f(x) = (g(x))^k$. Consider $ab \in (f)$. Then, a^k or $b^k \in (f)$. Conversely, suppose $g, h \mid f$ where g, h are irreducible. Then, there exists $q(x)$ ($g(x), q(x), h(x)$ are relatively prime) such that $(g(x))^a (h(x))^b q(x) \in (f)$ but $(g(x)^a)^k, \left((h(x))^b q(x)\right)^k \notin (f)$ for all $k \in \mathbb{N}$.
(b) For zero divisors $a + I, b + I \in R/I$, $(b + I)(a + I) = ba + I = I \implies ba \in I$. As $b \notin I$, we conclude that, if I is primary, there exists n such that $a^n \in I \implies (a + I)^n = I$. For the other direction, we note that if $ab \in I$ where $a, b \notin I$, then a, b are zero divisors in R/I. Hence, there exists n such that $(a + I)^n = I \implies a^n \in I$.

Problem 22. Show that if R is a noetherian ring and $I \subset R$ is an ideal, then R/I is also noetherian.

Solution 22. By **Problem 18**, the ideals of R/I are of the form K/I where $K \subseteq R$ is an ideal containing I. Call S the set of generators of K (note S has finite cardinality). By **Problem 17** of the previous chapter, it suffices to note K/I is generated by

$$\{k + I \in K/I |\ k \in S\}.$$

CHAPTER 3.3

Affine Varieties

Problem 1. Write $V(y-x^2) \cap V(y-x^2-x+1)$ in the form $V(I)$ for some ideal I of $\mathbb{C}[x,y]$. What is I? Interpret this geometrically.

Solution 1. $V(y-x^2) \cap V(y-x^2-x+1) = V((y-x^2)+(y-x^2-x+1)) = V((y-x^2, 1-x))$. Geometrically, this this is the intersection of parabolas $y = x^2$ and $y = x^2 + x - 1$.

Problem 2. Is every finite subset of $\mathbb{A}^n_{\mathbb{C}}$ an algebraic set? Is every finite subset of $\mathbb{A}^n_{\mathbb{R}}$ an algebraic set? Is every finite subset of $\mathbb{A}^n_{\mathbb{C}}$ the vanishing set of a set of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$?

Solution 2. We prove that every finite subset of $\mathbb{A}^n_k$ is algebraic. Consider the set $\{p_1, \ldots, p_m\}$, where $p_i = (a_{i,1}, \ldots, a_{i,n})$. Defining $I_i = (x_1 - a_{i,1}) + \cdots + (x_n - a_{i,n})$, we note

$$I = \prod_{i=1}^{m} I_i \implies V(I) = \bigcup_{i=1}^{m} V(I_i) = \{p_1, \ldots, p_m\}.$$

For the next part, we consider $\mathbb{A}^1_{\mathbb{C}}$ and the finite set $\{i\}$. Since $p(i) = 0$ and $p(x) \in R[x]$ implies $p(-i) = 0$ (by the *Complex Conjugate Root Theorem*), we note $\{i\}$ isn't algebraic.

Problem 3. Show that any line in $\mathbb{A}^n_{\mathbb{R}}$ is an algebraic set.

Solution 3. Note that a line in $A^n_{\mathbb{R}}$ refers to the solution of a system of equations of the form

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= d_1 \\ &\vdots \\ a_{n-1,1}x_1 + a_{n-1,2}x_2 + \cdots + a_{n-1,n}x_n &= d_n \end{aligned}$$

for $a_{i,j} \in \mathbb{R}$. I.e. a line must be

$$V\Big((a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n - d_1) \times \cdots \times (a_{n-1,1}x_1 + a_{n-1,2}x_2 + \cdots + a_{n-1,n}x_n - d_n)\Big).$$

Problem 4. Show that $\{z : |z| < 1\} \subset \mathbb{A}^1_{\mathbb{C}}$ is not an algebraic set.

Solution 4. We hope so show any infinite $S \subsetneq A^1_k$ isn't algebraic. Assuming the contrary, there exists $I \subset k[x]$ with $V(I) = S$. Then, for $f \in I$, $f(x) = 0$ for all $x \in S$. As all non-zero $f \in k[x]$ have finitely many roots, $I = \{0\} \implies V(0) = A^1_k = S$. (contradiction!)

Problem 5. Show that $\{x : x > 0\} \subset \mathbb{A}^1_{\mathbb{R}}$ is not an algebraic set.

Solution 5. See **Problem 4**.

Problem 6. Show that if V is any infinite subset of the parabola $V(y-x^2) \subset \mathbb{R}$, then $I(V) = (y-x^2)$. Moreover, show that for any finite subset $W \subset V(y-x^2)$, $I(W) \supsetneq (y-x2)$.

Solution 6. As $V \subset (y-x^2)$, $I(V) \supset I(y-x^2) = (y-x^2)$. For $f \in I(V)$, we write $f(x,y) = q(x,y)(y-x^2) + r(x)$. As $f(x,y) = 0$ for all $(x,y) \in V$, we note r is identically 0 as there exists infinitely many x for which $r(x) = 0$. If V is finite, call the distinct x-coordinates in V $\{a_1, \ldots, a_n\}$. Then, $r(x) = (x-a_1)\cdots(x-a_n) \in I(V)$ and $I(V) \neq (y-x^2)$.

Problem 7. Show that the parabola $y = x^2$ and the line $y = 0$ have isomorphic coordinate rings.

Solution 7. Let k be a field of infinite cardinality. Begin by noting $(y) \subset I(V(y))$. For $f \in I(V(y))$, write $f(x) = q(x)y + r(x)$, and note r is identically 0 since $V(y)$ is infinite. I.e. $I(V(y)) = (y)$. Now, we hope to show

$$\frac{k[x,y]}{(y-x^2)} \cong k[x] \cong \frac{k[x,y]}{(y)}.$$

Consider maps $\alpha : k[x,y] \to k[x]$ and $\beta : k[x,y] \to k[x]$ where $\alpha(f(x,y)) = f(x,x^2)$ and $\beta(f(x,y)) = f(x,0)$. Noting that $\ker(\alpha) = (y-x^2)$, $\ker(\beta) = (y)$, and $\alpha(f(x)) = \beta(f(x)) = f(x)$, the result follows from the *First Isomorphism Theorem*.

Problem 8. Find all maximal ideals in $\mathbb{Q}[x,y]$ containing x^2+y^2-25 and

a) y b) $y-3$ c) $y-5$ d) $y-2$ e) $y-7$

Solution 8.

a) $(x-5, y)$ and $(x+5, y)$
b) $(x-4, y-3)$ and $(x+4, y-3)$
c) $(x, y-4)$
d) $(x^2-21, 2)$
e) $(x^2+y^2-25, y-7)$

Problem 9. Prove Proposition 2.2: If $V \subseteq \mathbb{A}_k^n$ is any set of points, then $I(V)$ is an ideal of $k[x_1, \ldots, x_n]$.

Solution 9. For all $f, g \in I(V)$ and $h \in k[x_1, \ldots, x_n]$,

(Closure Under Addition) $$f(p) + g(x_1, \ldots, x_n) = 0 \implies f(p) + g(x_1, \ldots, x_n) \in I(V)$$

(Absorption) $$h(p)f(p) = h(p) \times 0 = 0 \implies h(p)f(p) \in I(V)$$

for all points $p \in V$.

Problem 10. Prove Proposition 2.6: Let V and W be algebraic sets.

(1) $I(V \cup W) = I(V) \cap I(W)$
(2) $I(V \cap W) = I(V) + I(W)$

Solution 10.

(1) Consider $f \in I(V \cup W)$. As f vanishes over both V and W, $f \in I(V) \cap I(W)$. Consider $g \in I(V) \cap I(W)$. As g vanishes over V and W, g vanishes over their union. I.e. $g \in I(V \cup W)$.
(2) We provide a counterexample. Consider $V = V(x^2+y^2)$ and $W = V(X^2-y^2)$.

$$I(V \cap W) = I(\{(0,0)\}) = (x,y) \neq I(V) + I(W) = (x^2+y^2) + (x^2-y^2) \subseteq (x^2, y^2)$$

since $x, y \notin (x^2, y^2)$.

Problem 11. Prove Theorem 2.4: If $X \subseteq \mathbb{A}^n$, then $X \subseteq V(I(X))$. If $S \subseteq k[x_1, \ldots, x_n]$, then $S \subseteq I(V(S))$.

Solution 11. By definition, $f \in I(X) \implies \forall x \in X,\ f(x) = 0$. Hence, $x \in V(I(X))$. Once again, by definition, $p \in V(S) \implies g(p) = 0 \forall g \in S$. Hence, $g \in I(V(S))$.

Problem 12. Show that $(xy-1) \subseteq \mathbb{R}[x, y]$ is a prime ideal. Show that $(xy-1) \subseteq \mathbb{C}[x, y]$ is also a prime ideal.

Solution 12. Consider the map $\phi : \mathbb{R}[x, y] \to \mathbb{R}\left[x, \frac{1}{x}\right]$. We note ϕ is a surjective homomorphism:

(Surjectivity) $$\phi(g(x, y)) = f\left(x, \frac{1}{x}\right) \implies g(x, y) = f(x, y)$$

(Multiplicative Homomorphism) $$\phi(g(x, y)f(x, y)) = g\left(x, \frac{1}{x}\right) f\left(x, \frac{1}{x}\right) = \phi(g(x, y))\phi(f(x, y))$$

(Additive Homomorphism) $$\phi(g(x, y) + f(x, y)) = g\left(x, \frac{1}{x}\right) + f\left(x, \frac{1}{x}\right) = \phi(g(x, y)) + \phi(f(x, y))$$

$$\phi(1) = 1$$

As $f(x, y)$ can be written as

$$f(x, y) = q(x, y)(xy - 1) + r(x),$$

$f\left(x, \frac{1}{x}\right) = 0 \implies r(x) = 0$. We conclude $\ker(\phi) = (xy - 1)$ and $\mathbb{R}[x, y]/(xy - 1) \cong \mathbb{R}\left[x, \frac{1}{x}\right]$ by the *First Isomorphism Theorem*. Noting $\mathbb{R}\left[x, \frac{1}{x}\right] \subset \mathbb{R}(x)$, we conclude $\mathbb{R}\left[x, \frac{1}{x}\right]$ is an integral domain (and $(xy - 1)$ is prime) from **Problem 3** of chapter one. Replacing the $\mathbb{R}$'s with $\mathbb{C}$'s, the second result follows.

Problem 13.

(a) We showed that $V(IJ) = V(I) \cup V(J)$. Show that $V(I \cap J) = V(I) \cup V(J)$ as well. Find an example of ideals in $k[x_1, \ldots, x_n]$ such that $IJ \neq I \cap J$, and conclude that different ideals can have the same vanishing sets.
(b) When do two ideals $I, J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ have the same vanishing sets?
(c) Suppose that $I, J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ have the same vanishing sets. Show that $V(I+J) = V(I) = V(J)$. Conclude that, for an algebraic set V , there is a largest possible ideal I so that $V = V(I)$.

Solution 13.

(a) Let $p \in V(I) \cup V(J)$. WLOG, $\forall f \in I,\ f(p) = 0$. As $I \cap J \subseteq I$, $p \in V(I \cap J)$. Conversely, suppose $p \notin V(I) \cup V(J)$. Then, $\exists f \in I$ and $\exists g \in J$ such that $f(p), g(p) \neq 0$. Then, $fg \in I \cap J$ and $f(p)g(p) \neq 0$. I.e. $p \notin V(I \cap J)$. Let our polynomial ring be $\mathbb{R}[x]$, and let $I = (x)$ and $J = (x^2)$. $IJ = (x^3)$ and $I \cap J = (x)$.
(b) By the Nullstellensatz, $\sqrt{I} = \sqrt{J}$.
(c) As $I \subseteq I + J$, $V(I + J) \subseteq V(I)$. Then, let $p \in V(I)$ (and, hence, $p \in V(J)$). For $f \in I$ and $g \in J$, $(f + g)(p) = f(p) + g(p) = 0 \implies p \in V(I + J)$. As $\mathbb{C}[x_1, \ldots, x_n]$ is noetherian, there exists a 'largest' ideal I such that $V(I) = V$: I.e. an ideal I such that if $I \subseteq I'$ and $V(I') = V(I) = V$, then $I = I'$. In the hope of proving the uniqueness of I, suppose an ideal J is also a 'largest' ideal of V. Then, $V(I) = V(J) = V \implies V(I + J) = V \implies I = I + J = J$.

Problem 14. The *twisted cubic* is the set $\{(t, t^2, t^3) : t \in \mathbb{C}\}$ in $\mathbb{A}^3$.

(a) Show that the twisted cubic is an algebraic set, by writing it as $V(I)$ for some ideal I of $\mathbb{C}[x, y, z]$.

(b) Show that the twisted cubic is isomorphic to $\mathbb{A}^1$.

Solution 14.

(a) $I = (y^2 - x, z^3 - x)$.

(b) Consider the morphisms
- $\phi : V(I) \to \mathbb{A}^1$, where $\phi((t, t^2, t^3)) = t$.
- $\psi : \mathbb{A}^1 \to V(I)$, where $\psi(t) = (t, t^2, t^3)$.

$(\phi \circ \psi)(t) = t$ and $(\psi \circ \phi)(t, t^2, t^3) = (t, t^2, t^3)$.

Problem 15. Let $X = V(x^2 - yz, xz - x) \subset A$. Write X as the union of several irreducible components.

Solution 15.

$$\begin{aligned} V(x^2 - yz, xz - x) &= V(x - yz) \cap V(xz - x) \\ &= V(x^2 - yz) \cap (V(z - 1) \cup V(x)) \\ &= V(x^2 - y, z - 1) \cup V(x, yz) \\ &= V(x^2 - y, z - 1) \cup V(x, y) \cup V(x, z) \end{aligned}$$

Problem 16. Let R be a ring. We say that an element $r \in R$ is nilpotent if there is some positive integer n such that $r^n = 0$. We say that R is a reduced ring if the only nilpotent element of R is 0.

(a) Show that the set of nilpotent elements of a ring R forms an ideal of R. We call this ideal the nilradical of R, and we denote it by $\mathfrak{N}(R)$.

(b) Show that $\mathfrak{N}(R)$ is the intersection of all the prime ideals of R.

(c) Show that if R is the coordinate ring of some algebraic set, then R is a reduced ring, i.e. $\mathfrak{N}(R) = (0)$.

(d) Find a ring R with $\mathfrak{N}(R) \neq (0)$.

Solution 16.

(a) Let $r, r' \in \mathfrak{N}(R)$ ($r^n = r^m = 0$) and $a \in R$. Then, $(ar)^n = a^n \times 0 = 0$, and, by the *Binomial Theorem*, $(r + r')^{m+n} = 0$.

(b) Suppose r is nilpotent and I is prime. By induction, we hope to show $r^n \in I \implies r \in I$. if $n = 1$, the result is apparent. For $n > 1$, $r^n \in I \implies r^{n-1} \in I$ or $r \in I$. If $r \in I$, we're done, and if $r^{n-1} \in I$, then, by the inductive hypothesis, we're done. Now, consider a non-nilpotent element a and the largest ideal $\mathfrak{m}$ not containing a^n for all positive integer n. Note that we can choose such $\mathfrak{m}$ by use of *Zorn's Lemma*. Striving for a contradiction, suppose $\mathfrak{m}$ isn't prime. Then, there exists $xy \in \mathfrak{m}$ where $x, y \notin \mathfrak{m}$. Noting $(x) + \mathfrak{m}$ and $(y) + \mathfrak{m}$ contain $\mathfrak{m}$, there exists p, q such that $a^p \in (a) + \mathfrak{m}$ and $a^q \in (b) + \mathfrak{p}$. Then, $a^{p+q} \in (ab) + \mathfrak{m} = \mathfrak{m}$ (contradiction!) Hence, $\mathfrak{m}$ is prime ideal, with $a \notin \mathfrak{m}$.

(c) Consider non-zero $f \in R = \mathcal{O}(V)$. As $f \neq 0$, $\exists p \in V$ such that $f(p) \neq 0$. Assuming f is nilpotent, $\exists n \in \mathbb{N}$ such that $(f(p))^n = 0$, contradicting that $k[x_1, \ldots, x_n]$ is an integral domain.

(d) Let $R = \mathbb{Z}/4\mathbb{Z}$. Note $2^2 \equiv 0 \pmod 4$.

Problem 17. We say that an algebraic set X is connected if whenever we write $X = Y \cup Z$ as a union of two algebraic sets which are disjoint, i.e. $Y \cap Z = \varnothing$, then either Y or Z is equal to X.

(a) Let R bearing. We say that an element $e \in R$ is an idempotent if $e^2 = e$. Find all the idempotent elements in the ring $\mathbb{C}[x]/(x^2 - x)$.

(b) Show that a ring R has idempotent elements other than 0 and 1 if and only if R is isomorphic to a direct product $R_1 \times R_2$ of nontrivial rings.

(c) Show that an algebraic set X is connected if and only if its coordinate ring $\mathcal{O}(X)$ has no idempotent elements other than 0 and 1.

Solution 17.

(a) Begin by noting that

$$\frac{\mathbb{C}[x]}{(x^2-x)} \cong \mathbb{C} \times \mathbb{C}$$

from **Problem 10** of the previous chapter. Then, note the zero divisors of $\mathbb{C} \times \mathbb{C}$ are of the form $(0,a)$ and $(b,0)$ for $a,b \in \mathbb{C}$. As $e^2 - e = 0 \implies e(e-1) = 0$, we note $e \in \{(1,1),(0,0),(1,0),(0,1)\}$. In our coordinate ring, these correspond to $\{1,0,x,1-x\}$.

(b) Consider the non-trivial idempotent elements $e, (1-e) \in R$. Let $R_1 = (e)$ and $R_2 = (1-e)$. e and $1-e$ are the respective identities of R_1 and R_2. Along with the properties R_1, R_2 inherit from being ideals, we may conclude R_1 and R_2 are rings. Define the map $f : R \to R_1 \times R_2$ such that $f(r) = (re, r(1-e))$. Consider $r_1, r_2, k \in R$.

(Additive Homomorphism) $$f(r_1 + r_2) = (r_1 e, r_1(1-e)) + (r_2 e, r_2(1-e)) = f(r_1) + f(r_2)$$

(Multiplicative Homomorphism) $$f(r_1 \times r_2) = (r_1 e, r_1(1-e)) \times (r_2 e, r_2(1-e)) = f(r_1) \times f(r_2)$$

$$f(1) = (e, (1-e))$$

$\ker(f) = 0$ since $ke = 0$ and $k(1-e) = 0$ implies $k - ke = k = 0$. $\text{im}(f) = R_1 \times R_2$ since $f(xe + y(1-e)) = (xe, y(1-e))$. For the opposite direction, note $(0,1) \in R_1 \times R_2$ is idempotent and not the additive or multiplicative identity.

(c) By the Nullstellensatz, $I(Y \cap Z) = \sqrt{I(Y) + I(Z)} = \mathbb{C}[x_1, \ldots, x_n]$. As $1 \in \sqrt{I(Y) + I(Z)}$, $1 \in I(Y) + I(Z) \implies I(Y) + I(Z) = \mathbb{C}[x_1, \ldots, x_n]$. Now, we apply the *Chinese Remainder Theorem* to note

$$\mathcal{O}(X) = \frac{\mathbb{C}[x_1, \ldots, x_n]}{I(Y) \cap I(Z)} \cong \frac{\mathbb{C}[x_1, \ldots, x_n]}{I(Y)} \times \frac{\mathbb{C}[x_1, \ldots, x_n]}{I(Z)} = \mathcal{O}(Y) \times \mathcal{O}(Z).$$

It follows that if X is disconnected, $\mathcal{O}(X)$ has non-trivial idempotent elements by part (b). Now, suppose there exists a non-trivial idemptotent element $f \in \mathcal{O}(X)$. Note that $\forall p \in X$, $(f(p))^2 = f(p) \implies f(p) \in \{0,1\}$. Then, define $Y = X \cap V(f)$ and $Z = X \cap V(f-1)$ to note X is disconnected.

Problem 18. We saw that the union of two (and hence any finite number of) algebraic sets in $\mathbb{A}^n_k$ is algebraic. Give an example to show that the union of infinitely many algebraic sets need not be algebraic. On the other hand, show that an intersection of infinitely many algebraic sets is always algebraic.

Solution 18. Consider the non-algebraic set

$$V = \bigcup_{\substack{x \in \mathbb{C} \\ |x|<1}} \{x\} \subseteq \mathbb{A}^1_{\mathbb{C}}.$$

See **Problem 4** for a proof. Now, suppose the set S consists of infinitely many algebraic subsets of $\mathbb{A}^n_k$ and S' consists of their corresponding ideals. We hope to show

$$\bigcap_{V \in S} V = V\left(\bigcup_{J \in S'} J\right).$$

Suppose $p \in V\left(\bigcup_{J \in S'} J\right)$. Then, for all $f \in \bigcup_{J \in S'} J$, $f(p) = 0$. I.e. $p \in V(J)$ for all $J \in S'$ and, hence, $p \in \bigcap_{V \in S} V$. Suppose $p \notin V\left(\bigcup_{J \in S'} J\right)$. Then, there exists $J \in S'$ and $f \in J$ such that $f(p) \neq 0$. As $\bigcap_{V \in S} V \subseteq V(J)$, $p \notin \bigcap_{V \in S} V$.

CHAPTER 3.4

Hilbert's Nullstellensatz

Problem 1. For a field k, not necessarily algebraically closed, and positive integers m and n, let $I = (x^m, y^n)$ be an ideal of $k[x, y]$. Show that $\sqrt{I} = (x, y)$.

Solution 1. Consider $f(x, y)x + g(x, y)y \in (x, y)$. By the *Binomial Theorem*,

$$(f(x, y)x + g(x, y)y)^{m+n} \in I \implies f(x, y)x + g(x, y)y \in \sqrt{I}.$$

Suppose $h(x, y) \notin I$. Then, the constant term (the coefficient of x^0y^0) of h is non-zero. Then, $(h(x))^n \notin I \forall n \in \mathbb{N}$.

Problem 2. Let $f, g \in k[x, y]$ be distinct non-constant polynomials. Is it necessarily true that $\sqrt{(f^2, g^3)} = (f, g)$? Prove or give a counterexample.

Solution 2. By **Problem 1**, set $f = x^2$ and $g = y^2$ to obtain a counterexample.

Problem 3. Show that if R is any ring and $I \subset R$ is an ideal, then $\sqrt{I}$ is a radical ideal.

Solution 3. We begin by showing $\sqrt{I}$ is an ideal. Suppose $a, b \in \sqrt{I} \implies \exists m, n,\ a^n, b^m \in I$ and $r \in R$.

- $(ra)^n = r^n a^n \in I$.
- $(a + b)^{n+m} \in I$ by the *Binomial Theorem*.

Problem 4. For which rings R is (0) a radical ideal? For which positive integers n is (0) a radical ideal of $\mathbb{Z}/n\mathbb{Z}$?

Solution 4. (0) is a radical ideal in R when R is reduced. I.e. it has no nilpotent elements. $\mathbb{Z}/n\mathbb{Z}$ is reduced when n is square free.

Problem 5. Let $I = (x^2 + y^2 - 1, y - 1) \subset \mathbb{C}[x, y]$. Find, with proof, an element of $I(V(I)) \setminus I$.

Solution 5. Consider $h(x, y) = x + y - 1$. As h vanishes over $V(I) = \{(0, 1)\}$, $h \in I(V(I))$. Suppose $h(x) = f(x)(x^2+y^2-1)+g(x)(y-1)$. As $\deg h < \deg f$ in $(\mathbb{C}[x])[y]$, $f(x) = 0$. Then, since $y-1 \nmid x+y-1$, the result follows.

Problem 6. Let $p, q \in \mathbb{C}[x, y]$. Show that $V(p) = V(q)$ if and only if $p \mid q^n n$ for some n and $q \mid p^m$ for some m. Show that this is false over a non-algebraically closed field.

Solution 6. By the *Nullstellensatz*,

$$V(p) = V(q) \implies \sqrt{(p)} = I(V(p)) = I(V(q)) = \sqrt{(q)}.$$

The desired result follows.

Problem 7. Let $X = V(x^2+y^2-1, z^2+x^3+y^3-1) \subset \mathbb{A}^3_{\mathbb{C}}$ and $Y = V(x^2+y^2-1) \subset \mathbb{A}^2_{\mathbb{C}}$. Let $f : X \to Y$ be defined by $f(a,b,c) = (a,b)$. Describe explicitly the induced map $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Solution 7. $\phi(g) = g \circ f(a,b,c) = g(a,b)$.

Problem 8. Let $\phi : k[x,y,z]/(xy-1, z-x^2+y^2) \to k[t]$ be defined by $\phi(x) = 1$, $\phi(y) = 1$, and $\phi(z) = 0$. Describe the induced map from $\mathbb{A}^1_k$ to $(xy-1, z-x^2+y^2) \subset \mathbb{A}^3_k$.

Solution 8. Call the map ψ. Then, $\psi(t) = (\phi(x)(t), \phi(y)(t), \phi(z)(t)) = (1,1,0)$.

Problem 9. If R is any ring and I any ideal, show that $\sqrt{I}$ is the intersection of the prime ideals containing I.

Solution 9. Suppose $p \in \sqrt{I}$. Then, $p^m \in I$, and, for $\mathfrak{p} \supset I$, $p^m \in \mathfrak{p} \implies p \in \mathfrak{p}$ by induction. Now, suppose $q \notin \sqrt{I}$. Call S the set of ideals J contain I such that $q \notin \sqrt{J}$. With a partial order of inclusion, we apply *Zorn's Lemma* to choose a maximal element $\mathfrak{q} \in S$. It suffices to show $\mathfrak{q}$ is prime. Suppose $a, b \notin \mathfrak{q}$. As $(a)+\mathfrak{q}, (b)+\mathfrak{q} \notin S$, $q^m = ka + c$ and $q^n = k'b + c'$ for $c, c' \in \mathfrak{q}$, $k, k' \in R$, and $m, n \in \mathbb{N}$. Then,

$$x^{m+n} = kk'ab + kac' + k'bc + cc' \in (ab) + \mathfrak{q}.$$

We conclude $(ab) + \mathfrak{q} \neq \mathfrak{q} \implies ab \notin \mathfrak{q}$.

Problem 10. Show that if $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is an ideal, then $\sqrt{I}$ is the intersection of the maximal ideals containing I.

Solution 10. Call S the set of maximal ideals containing I. Then, it suffices to show

$$V\left(\bigcap_{\mathfrak{m} \in S} \mathfrak{m}\right) = \bigcup_{\mathfrak{m} \in S} V(\mathfrak{m}) = V(I).$$

Indeed, by the *Nullstellensatz*, $\bigcap_{\mathfrak{m}\in S} \mathfrak{m} = I\left(\bigcup_{\mathfrak{m}\in S} V(\mathfrak{m})\right) = I(V(I)) = \sqrt{I}$. As maximal ideals are prime, **Problem 9** provides us the first inclusion for free: $\bigcup_{\mathfrak{m}\in S} V(\mathfrak{m}) \subset V(I)$. Consider the point $p = (a_1, \ldots, a_n)$ and its associated maximal ideal $\mathfrak{n} = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$. $V(\mathfrak{n}) = \{p\} \subset V(I) \implies \mathfrak{n} \supset \sqrt{I} \supset I$. Then, $\mathfrak{n} \in S$, and the desired result follows.

Problem 11. Show that $\sqrt{(x^2 - 2xy^4 + y^6, y^3 - y)} \subset \mathbb{C}[x,y]$ is the intersection of three maximal ideals. What are they? Can you somehow "see" that $(x^2 - 2xy^4 + y^6, y^3 - y)$ is not a radical ideal?

Solution 11.

$$\implies V(x^2 - 2xy^4 + y^6, y^3 - y) = \{(0,0), (1,1), (1,-1)\} = V((x,y) \cap (x-1, y-1) \cap (x-1, y+1))$$
$$\implies \sqrt{(x^2 - 2xy^4 + y^6, y^3 - y)} = (x,y) \cap (x-1, y-1) \cap (x-1, y+1).$$

We note $x(x-1)(y-1) \in \sqrt{I}$ but $x(x-1)(y-1) \notin I$ by comparing degrees in $(\mathbb{C}[x])[y]$.

Problem 12. Show that the semialgebraic sets in $\mathbb{A}^1_{\mathbb{R}}$ are finite unions of points and closed intervals (bounded or unbounded).

Solution 12. Consider the semialgebraic set $S = \{p \in \mathbb{A}^1_{\mathbb{R}} |\ g_1(p), g_2(p), \ldots, g_(n) \geq 0\}$. Then,

$$S = S_1 \cap S_2 \cap \cdots \cap S_m,$$

where $S_i = \{p \in \mathbb{A}^1_{\mathbb{R}} |\ g_i(p) \geq 0\}$. Since g_i has finitely many roots, S_i is the finite union of closed sets or points. Since $\cap$ is distributive over $\cup$, our result follows from Lemma 0.1.29.

Problem 13. Use the *Chevalley-Warning Theorem* to show that a quadratic form in $n \geq 3$ variables has a nontrivial zero (i.e. other than $(0, 0, \ldots, 0)$) in $\mathbb{A}^n_{\mathbb{F}_p}$. Find a quadratic form in two variables that does not have a nontrivial zero in $\mathbb{A}^2_{\mathbb{F}_p}$.

Solution 13. Consider the quadratic form f. As $f(0, 0, \ldots, 0) = 0$ and $n > \deg f = 2$, the *Chevalley-Warning Theorem* guarantees f has a non-trivial root. Suppose p is an odd prime congruent to 3 modulo 4. Then, $x^2 + y^2$ has no non-trivial roots in $\mathbb{A}^2_{\mathbb{F}_p}$.

Problem 14. Let $M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$ be Motzkin's polynomial.

a) Show that $M(x, y)$ is a nonnegative polynomial on $\mathbb{A}^2_{\mathbb{R}}$.
b) Show that $M(x, y)$ cannot be written as a sum of squares of polynomials.

Solution 14.

a) As $M(x, y) = M(-x, y) = M(x, -y) = M(-x, -y)$, we suppose $x, y \geq 0$. By the *AM-GM Inequality*,

$$\frac{x^4y^2 + x^2y^2 + 1}{3} \geq \sqrt[3]{x^6y^6} = x^2y^2 \implies M(x, y) \geq 0.$$

b) Suppose M can be written as the sum of squares. I.e. $M(x, y) = (ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j)^2 + (a'x^3 + b'x^2y + c'xy^2 + d'y^3 + e'x^2 + f'xy + g'y^2 + h'x + i'y + j')^2$. By expanding, $a = d = e = g = h = i = a' = d' = e' = g' = h' = i' = 0$. Then, we note the coefficient of x^2y^2 is $f^2 + (f')^2 > -3$. (contradiction!)

Problem 15. Show that if $f(x) \in \mathbb{R}[x]$ is a polynomial in a single variable which is positive on all of $\mathbb{R}$, then f can be written as a sum of squares of polynomials.

Solution 15. As f is positive, f is the product of irreducible quadratics in $R[x]$. By Lemma 0.1.28, it suffices to show irreducible quadratics are the sum of squares. Consider $ax^2 + bx + c$, where $b^2 - 4ac < 0$ and $a > 0$. Then,

$$ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a} = \left(\sqrt{a}\left(x + \frac{b}{2a}\right)\right)^2 + \left(\sqrt{c - \frac{b^2}{4a}}\right)^2.$$

Problem 16. Generalize the *Erdős-Ginzburg-Ziv Theorem* to the case where n is composite.

Solution 16. It suffices to show that if the *Erdős-Ginzburg-Ziv Theorem* holds for p, q, then it holds for pq. By induction, the result then follows for all composite n. Consider an arbitrary set S of $2pq - 1$ elements in $\mathbb{Z}$. As the *Erdős-Ginzburg-Ziv Theorem* holds for p, choose p elements $a_{1,1}, a_{2,1}, \ldots, a_{p,1} \in S$ who's sum is divisible by p. Eliminating these elements from S and repeating the same procedure $2q - 1$ times, we

construct $2q-1$ sums:

$$\begin{aligned} a_{1,1}+a_{2,1}+\cdots+a_{p,1}&=a_1\\ a_{1,2}+a_{2,2}+\cdots+a_{p,2}&=a_2\\ &\vdots\\ a_{1,2q-1}+a_{2,2q-1}+\cdots+a_{p,2q-1}&=a_{2q-1}\end{aligned}$$

As the *Erdős-Ginzburg-Ziv Theorem* holds for q, choose q elements $a_{j_1}, a_{j_2}, \ldots, a_{j_q} \in \{a_1, a_2 \ldots, a_{2q-1}\}$. Then, we note

$$\sum_{i=1}^{q} a_{j_i} = \sum_{i=1}^{q}\sum_{s=1}^{p} a_{s,j_i}$$

is divisible by pq to obtain the desired result.

Problem 17. Suppose that m hyperplanes in $\mathbb{R}^n$ contain all but one of the vertices of an n-dimensional hypercube with vertices $\{0,1\}^n$. Show that $m \geq n$.

Solution 17. Suppose $m < n$ and consider the m hyperplanes $f_1, f_2, \ldots, f_m$. Call $(a_1, \ldots, a_n)$ the vertex not contained in $\bigcup_{i=1}^{m} V(f_i)$ and let $\overline{a_j} = 1 - a_j$. Then, define

$$f = \prod_{i=1}^{m} f_i + \delta \prod_{j=1}^{n} (x_j - \overline{a_j}),$$

where δ is chosen such that $f(a_1, \ldots, a_n) = 0$. Note δ must be non-zero. Then, deg $f = n$ and lead $f = \delta x_1 x_2 \cdots x_n$. Then, we contradict the *Combinatorial Nullstellensatz* as f must be non-zero somewhere in $\{0,1\}^n$.

Problem 18. Let n be a positive integer. Consider

$$S = \{(x,y,z) |\ x,y,z \in \{0,1,\ldots,n\}, x+y+z > 0\}.$$

as a set of $(n+1)^3 - 1$ points in three-dimensional space. Determine the smallest possible number of planes, the union of which contains S but does not include $(0,0,0)$. (IMO 2007)

Solution 18. We consider the two dimension analogue of this question to obtain some intuition.

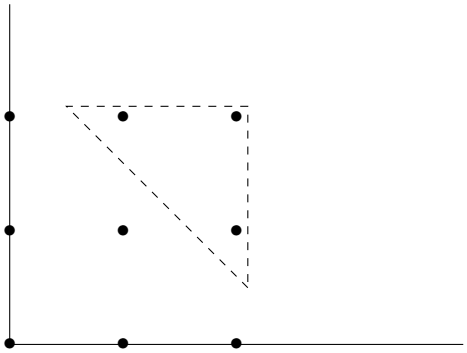


FIGURE 1. Points in $\mathbb{R}^2$ $(n = 2)$

In particular, what is the smallest number of lines who's union passes through $S = \{(x,y) |\ x,y \in \{0,1,\ldots,n\}, x+y > 0\}$? Intuitively, we can see that if a line passes through a point on either axis and a point in the triangle, it doesn't pass through any point on the other axis, and, similarly, if a line were to pass through two of the

axes, it couldn't pass through the triangle if none of the lines passed through $(0,0)$. Then, we'd need a minimum of $2n$ lines. $2n$ is also the best bound since we could simply consider the lines $x = 1, x = 2, \ldots, x = n$ and $y = 1, y = 2, \ldots, y = n$. Coming back to the three dimensional case, we hope to show we need a minimum of $3n$ planes. Suppose the result was false. I.e. there exists planes $f_1, f_2, \ldots, f_m$ with $m < 3n$ that satisfy the constraints of the problem. Then, define

$$f = \left(\prod_{i=1}^{m} f_i\right) + \left(\delta \times \prod_{j \in \{x,y,z\}} \prod_{i=1}^{n} (j - i)\right),$$

where δ is chosen such that $f(0, 0, \ldots, 0) = 0$. Note δ is non-zero. Then, deg $f = 3n$ and lead $f = \delta x^n y^n z^n$. Then, we contradict the *Combinatorial Nullstellensatz* as f must be non-zero somewhere in $\{0, \ldots, n\} \times \{0, \ldots, n\} \times \{0, \ldots, n\} = S$.

CHAPTER 3.5

Localization

Problem 1. Describe the ideals of the rings $\mathbb{C}[x]_{(x)}$ and $\mathbb{C}[x]\left[\frac{1}{x^2+x}\right]$.

Solution 1. The ideals of $\mathbb{C}[x]_{(x)}$ are those of the form (x^n) for $n \in \mathbb{N}$. The ideals of $\mathbb{C}[x]\left[\frac{1}{x^2+x}\right]$ are those of the form $(f(x))$ where f is not a power of $(x+1)$ or x. Two ideals $(f), (g)$ are the same when f and g differ by a factor of $x^i(x+1)^j$ for $i, j \in \mathbb{Z}$.

Problem 2. Find a local ring whose ideals do not form a chain.

Solution 2. Consider the local ring $\mathbb{C}[x,y]_{(x,y)}$ and the ideals (x) and (y). We note $(x) \not\subseteq (y)$ since

$$\frac{x}{1} = \frac{yf(x,y)}{g(x,y)} \iff xg(x,y) = yf(x,y) \implies y \mid g(x,y) \text{ (contradiction!)}$$

Applying a similar argument to show $(y) \not\subseteq (x)$, the result follows.

Problem 3. Describe all the ideals and units of the following rings:

a) $\mathbb{Z}\left[\frac{1}{60}\right]$
b) $\mathbb{Z}_{(3)}$
c) $\mathbb{C}[x,y]_(x)$

Solution 3.

a) The units of $\mathbb{Z}\left[\frac{1}{60}\right]$ are $\frac{d}{60^n}$, where d is the product of powers of divisors of 60 and $n \in \mathbb{N}$. Then, the ideals of $\mathbb{Z}\left[\frac{1}{60}\right]$ are of the form (a) for $a \in \mathbb{Z}$. Note $(a) = (b)$ iff a and b differ by units.
b) The units of $\mathbb{Z}_{(3)}$ are of the form $\frac{a}{b}$ where $3 \nmid a$. The ideals are then precisely of the form (3^n) for $n \in \mathbb{N}$.
c) The units of $\mathbb{C}[x,y]_(x)$ are of the form $\frac{a}{b}$, where $x \nmid a$. Similarly, the ideals are of the form (x^n) for $n \in \mathbb{N}$.

Problem 4. Show that if R is a Principle Ideal Domain, then any localization of R is also a Principle Ideal Domain.

Solution 4. Consider an ideal I of $S^{-1}R$. Since

$$\frac{x}{y} \in I \iff x \in I,$$

it follows that the principle ideal $I \cap R$ of R generates I. It follows that I is principle.

Problem 5. Describe the coordinate ring of $\mathbb{A}^1 \setminus \{0\}$. What about $\mathbb{A}^1 \setminus \{a_1, \ldots, a_n\}$, where $a_1, \ldots, a_n$ are distinct points in $\mathbb{A}^1$?

Solution 5.

$$\mathcal{O}(\mathbb{A}^1 \setminus \{a_1, \ldots, a_n\}) = \mathbb{C}\left[x, \frac{1}{(x-a_1)\cdots(x-a_n)}\right].$$

Problem 6. Prove Proposition 2.3: Let $\phi : R \to S^{-1}R$ be the localization homomorphism.

- $\ker(\phi) = \{r \in R |\ sr = 0 \text{ for some } s \in S\}$.
- $S^{-1}R = \{0\}$ if and only if $0 \in S$.

Solution 6. The first follows from noting

$$\frac{r}{s'} = \frac{0}{1} \iff \exists s \in S,\ s(r \cdot 1 - s' \cdot 0) = sr = 0.$$

For the second, $0 \in S \implies 0 \times (r \cdot 1 - s \cdot 0) = 0 \iff \frac{r}{s} = \frac{0}{1}$. For the reverse direction, we note $\frac{1}{1} = \frac{0}{1} \iff \exists s \in S,\ s(1 \cdot 1 - 0 \cdot 1) = 0 \implies s = 0$.

Problem 7. Complete the proof of Proposition 2.4: Let R be a ring and S a multiplicative subset. Then, there is a bijection between the set of prime ideals of $S^{-1}R$ and the set of prime ideals of R which do not intersect S.

Solution 7. We define our map from the set of prime ideals of $S^{-1}R$ to those of R that do not intersect S via the localization homomorphism ϕ. I.e. $\mathfrak{B} \to \phi^{-1}(\mathfrak{B}) = \mathfrak{B}^c$. We define our inverse map such that prime $\mathfrak{p}$ is sent to it's localization under S. I.e. $\mathfrak{p} \to S^{-1}\mathfrak{p} = \mathfrak{p}^e$.

(1) As ϕ is a homomorphism, $\mathfrak{B}^c$ is prime.
(2) Suppose $s \in \mathfrak{B}^c \cap S$. Then, we contradict the primality of $\mathfrak{B}$ as $\mathfrak{B}$ has a unit.
(3) Suppose $\frac{a}{s_1}\frac{b}{s_2} \in \mathfrak{p}^e$. Then, $ab \in \mathfrak{p}$. WLOG, $a \in \mathfrak{p}$, and, hence, $\frac{a}{s_1} \in \mathfrak{p}^e$.
(4) We note
$$(\mathfrak{p}^e)^c = \phi^{-1}(S^{-1}\mathfrak{p}) = \left\{r \in R \middle|\ \frac{r}{1} \in S^{-1}\mathfrak{p}\right\}.$$
As $\frac{r}{1} = \frac{p}{s} \iff rss' = ps'$ for $s, s' \in S, p \in \mathfrak{p}$, we note $r \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and intersects S trivially. The other inclusion follows for free. In other works, $(\mathfrak{p}^e)^c = \mathfrak{p}$. Then, note $(\mathfrak{B}^c)^e = S^{-1}\phi^{-1}(\mathfrak{B})$. Since
$$\frac{r}{s} \in \mathfrak{B} \iff \frac{r}{1} \in \mathfrak{B} \iff r \in \phi^{-1}(\mathfrak{B}),$$
our desired inclusions follow. I.e. $(\mathfrak{B}^c)^e = \mathfrak{B}$.

Problem 8. Prove Proposition 5.2: Let V be a variety, and let $p \in V$. The stalk $\mathcal{O}_p(V)$ at p is a local ring. Its (unique) maximal ideal is $\mathfrak{m}_p = \{f \in \mathcal{O}_p(V) |\ f(p) = 0\}$.

Solution 8. We define our ring such that $(f, X) + (g, Y) = (f + g, X \cap Y)$ and $(f, X) \times (g, Y) = (fg, X \cap Y)$. Naturally, the additive identity is $(0, X)$, and the multiplicative identity is $(1, X)$. The ring axioms follow easily from the properties of $k(V)$. Now, it suffices to show the units are precisely the equivalence classes where $f(p) \neq 0$. If $f(p) = 0$, it's apparent f is a non-unit. Assuming $f(p)$ is non-zero, we can choose an open set U for which f doesn't vanish. Then, $(f, U) \times \left(\frac{1}{f}, U\right) = (1, U)$.

CHAPTER 3.6

Singular Points and Integrality

Problem 1. Determine whether the following are integral elements over the given rings:

(a) 4 over $\mathbb{Z}$
(b) $\frac{1}{3}$ over $\mathbb{Z}$
(c) $\frac{1}{3}$ over $\mathbb{Z}_{(5)}$
(d) $\frac{1}{x}$ over $\mathbb{C}[x]$
(e) $\sqrt{x^3+7x+4}$ over $\mathbb{C}[x]$
(f) $\frac{1+\sqrt{-7}}{2}$ over $\mathbb{Z}$
(g) $\frac{1+\sqrt{-5}}{2}$ over $\mathbb{Z}$

Solution 1. For the integral elements, we simply provide their associated polynomials.

(a) $x-4$
(b) $3x-1$ is the minimal polynomial of $\frac{1}{3}$ over $\mathbb{Z}$. By **Problem 2**, we conclude $\frac{1}{3}$ is non-integral over $\mathbb{Z}$.
(c) $x-\frac{1}{3}$
(d) $\frac{1}{x}$ is non-integral over $\mathbb{C}[x]$ by Lemmas 0.1.24 and 0.1.31.
(e) t^2-x^3-7x-4
(f) x^2-x+2
(g) $2x^2-2x+3$ is the minimal polynomial of $\frac{1+\sqrt{-5}}{2}$ By **Problem 2** (or, alternatively, **Problem 3**), we conclude $\frac{1}{3}$ is non-integral over $\mathbb{Z}$.

Problem 2. Show that if $m(x) \in \mathbb{Q}[x] \setminus \mathbb{Z}[x]$ is a monic polynomial and $g(x) \in \mathbb{Q}[x]$ is a monic polynomial, then $m(x)g(x) \notin \mathbb{Z}[x]$.

Solution 2. Let

$$m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and $i = \max\{i \in \mathbb{N} |\ a_i \in \mathbb{Q} \setminus \mathbb{Z}\}$. Suppose $\deg g = m$. Begin by choosing $\alpha \in \mathbb{Z}$ such that $g\prime(x) = \alpha g(x) \in \mathbb{Z}[x]$. Then, the coefficient of the x^{i+m} in $m(x)g\prime(x)$ is not in $\mathbb{Z}$ and, hence, $m(x)g(x) \notin \mathbb{Z}[x]$.

Problem 3. Let d be a squarefree integer. Compute the integral closure of $\mathbb{Z}$ in $Q(\sqrt{d})$.

Solution 3. Call the S the integral closure. Consider $a+b\sqrt{d}$, with $a, b \in \mathbb{Q}$ and $b \neq 0$. Then, our minimal polynomial f over $\mathbb{Q}$ is

$$f(x) = (x-a)^2 - b^2 d = x^2 - 2ax + a^2 - b^2 d.$$

By **Problem 2**, our problems reduces to determining $a, b \in \mathbb{Q}$ for which $2a, a^2 - b^2 d \in \mathbb{Z}$. We note $\mathbb{Z}[\sqrt{d}] \subseteq S$. In some cases, the reverse inclusion holds but, as we'll soon see, this isn't true in general. Since, $-2a \in \mathbb{Z}$, $a = \frac{n}{2}$ for $n \in \mathbb{Z}$. If n is even, $a \in \mathbb{Z}$ and, hence, $b \in \mathbb{Z}$ since d is squarefree. Suppose n is odd. Then,

$$a^2 - b^2 d = \frac{n^2}{4} - b^2 d \in \mathbb{Z} \implies \exists \text{ odd } m \in \mathbb{Z},\ b = \frac{m}{2}.$$

This implication follows from noting b^2d has a denominator of 4 and d is squarefree. Then,

$$a + b\sqrt{d} = \frac{1+\sqrt{d}}{2} + \frac{n-1}{2} + \frac{m-1}{2}\sqrt{d}.$$

Since the integral closure is always a ring, our problem reduces to determining if $\frac{1+\sqrt{d}}{2}$ is integral over $\mathbb{Z}$. In this case, $f(x) = 4x^2 - 4x + 1 - d$. We then conclude

$$S = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}.$$

Problem 4. Let i and j be relatively prime positive integers. Compute the integral closure of the ring $\mathbb{C}[x, y]/(x^i - y^j)$. What happens if $\gcd(i, j) > 1$?

Solution 4. Note by Lemma 0.1.32, $\mathcal{O}(X) = \mathbb{C}[x, y]/(x^i - y^j)$, where $X = V(x^i - y^j)$. Equivalently, we compute $\widetilde{X}$ and note $\mathcal{O}(\widetilde{X})$ is our desired integral closure. We hope to show $\widetilde{X} = \mathbb{A}^1$. Consider the maps

$$\phi : \mathbb{A}^1 \to X \text{ such that } \phi(t) = (t^j, t^i) \tag{31}$$

$$\psi : X \to \mathbb{A}^1 \text{ such that } \phi(x, y) = x^b y^a, \tag{32}$$

where a, b are chosen such that $ai + bj = 1$. Since ϕ and ψ are inverses everywhere expect the points corresponding to $(0, 0)$, the result follows.

Problem 5. For each of the following curves and points in $\mathbb{A}^2$, determine whether the curve is smooth or singular at the point. Sketch the curves to verify that the definition of smoothness is capturing the desired geometric property. For the ones that are singular, describe the type of singularity at the point.

(1) $V(y - x^2)$ at $(2, 4)$
(2) $V(y^2 - x^5)$ at $(0, 0)$
(3) $V(x^3 + y^3 - 3xy)$ at $(0, 0)$
(4) $V((y^2 - x^2)(x - 1)(2x - 3) - 4(x^2 + y^2 - 2x)^2)$ at $(1, 1)$
(5) $V(x^4 + x^2y^2 + y^4 - x(x^2 + y^2))$ at $(0, 0)$
(6) $V((x^2 + y^2)^2 - 3x^2 - y^2)$ at $(0, 0)$
(7) $V((x^2 + y^2)^2 - 3x^2 - y^2)$ at $(0, 1)$

Solution 5. We check if $f(x, y)$ has a singularity at (a, b) by seeing if $f(x + a, y + b)$ has a non-zero linear term.

(1) Since $y + 4 - (x + 2)^2 = y - x^2 - 4x$, our curve is smooth at $(2, 4)$
(2) Since $y^2 - x^5$ has no linear term, note that it's singular at $(0, 0)$. In particular, the singularity is a spinode.
(3) Once again, since $x^3 + y^3 - 3xy$ has no linear term, we note that it's singular at $(0, 0)$. In particular, the singularity is an crunode.
(4) Since

$$\begin{aligned} &= ((y+1)^2 - (x+1)^2)(x+1-1)(2(x+1)-3) - 4((x+1)^2 + (y+1)^2 - 2(x+1))^2 \\ &= -4((x+1)^2 + (y+1)^2 - 2(x+1))^2 \\ &= -4x^4 - 16x^2y - 16y^2 - 8x^2y^2 - 16y^3 - 4y^4, \end{aligned}$$

our curve has a singularity at $(1, 1)$, specifically a spinode.
(5) Since $x^4 + x^2y^2 + y^4 - x(x^2 + y^2)$ has no linear term, we note that it's singular at $(0, 0)$ and has a cusp there.
(6) Since $(x^2 + y^2)^2 - 3x^2 - y^2$ has no linear term, we conclude that it's singular at $(0, 0)$ and has an acnode there.

(7) Since

$$\begin{aligned}&= (x^2 + (y+1)^2)^2 - 3x^2 - (y+1)^2\\ &= x^4 + 2x^2y^2 + 4x^2y - x^2 + y^4 + 4y^3 + 5y^2 + 2y,\end{aligned}$$

our curve is smooth at $(0, 1)$.

Problem 6. Find an isomorphism between the rings $\mathbb{C}[x, y]/(y^2 - x^3)\left[\frac{1}{x}\right]$ and $\mathbb{C}\left[t, \frac{1}{t}\right]$.Similarly, find an isomorphism between the rings $\mathbb{C}[x, y]/(y^2 - x^2 - x^3)\left[\frac{1}{x}\right]$ and $\mathbb{C}\left[t, \frac{1}{t-1}, \frac{1}{t+1}\right]$.

Solution 6. Consider the surjective homomorphism $\phi : \mathbb{C}[x, y] \to \mathbb{C}[t^2, t^3]$, defined by $\phi(x) = t^2$ and $\phi(y) = t^3$. We hope to show $\ker(\phi) = (y^2 - x^3)$. We obtain one inclusion for free: $\ker(\phi) \subseteq (y^2 - x^3)$. For the other, consider f such that $\phi(f) = 0$. Applying the division algorithm in $\mathbb{C}[y]$, we write $f(x) = q(x)(y^2-x^3)+r(x, y)$, where r has degree one when treated as a polynomial in $\mathbb{C}[y]$. Let

$$r(x) = a + bx + cx^2 + \cdots + b'xy + c'x^2y + \cdots .$$

Then, $\phi(r) = a + bt^2 + cx^4 + \cdots + b't^5 + c't^7 + \cdots = 0 \implies r(x) = 0$. By the *First Isomorphism Theorem*, we conclude

$$\mathbb{C}[x, y]/(y^2 - x^3) \cong \mathbb{C}[t^2, t^3].$$

Hence, $\mathbb{C}[x, y]/(y^2 - x^3)\left[\frac{1}{x}\right] \cong \mathbb{C}\left[t^2, t^3, \frac{1}{t^2}\right] = \mathbb{C}\left[t, \frac{1}{t}\right]$. Applying a similar argument, we construct a surjective homorphism $\psi : \mathbb{C}[x, y]\left[\frac{1}{x}\right] \to \mathbb{C}\left[t(t^2 - 1), t^2 - 1, \frac{1}{t^2-1}\right]$, defined such that $\psi(y) = t(t^2 - 1)$ and $\psi(x) = t^2 - 1$. Noting that $\ker(\psi) = (y^2 - x^2 - x^3)$, we construct the desired isomorphism.

Problem 7. Let R be a ring, and let α be integral over R. Show that there exists finitely many elements $a_1, \ldots, a_n$ such that every element of $R[\alpha]$ can be written in the form $a_1r_1+\cdots+a_nr_n$ for some $r_1, \ldots, r_n \in R$. Show conversely that if $R[\alpha]$ is finitely generated as an R-module, then α is integral over R.

Solution 7. As α is integral over R, there exists monic $f \in R[x]$ such that $f(\alpha) = 0$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and, hence, deg $f = n$. Now, given a polynomial in α with degree $m > n-1$, we use that $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots+a_0$ to write g as a polynomial with degree $m-1$. We may repeat this process until g no longer has degree greater than $n - 1$. Hence, we conclude setting $r_i = \alpha^{i-1}$ satisfies the given constraints. To conclude the converse, suppose α is not integral. Then, given any finite set of polynomials $\{f_1, f_2, \ldots, f_m\}$ in α, consider

$$n = \max\{n \in \mathbb{N} |\ \exists i \in \{1, \ldots, m\},\ n = \deg f_i\}.$$

Then, α^{n+1} cannot be written as linear combination of f_i's.

Problem 8. Suppose that R and S are integral domains, and S is an integral extension of R. Show that R is a field if and only if S is a field.

Solution 8. For the first direction, consider $y \in S$. Then, there exists $r_0, \ldots, r_{n-1} \in R$ such that $y^n + r_{n-1}y^{n-1} + \cdots + r_0 = 0$. We may then conclude

$$\frac{1}{y} = -\frac{1}{r_0}y^{n-1} - \frac{r_{n-1}}{r_0}y^{n-2} - \cdots - \frac{r_1}{r_0}.$$

For the reverse direction, consider $x \in R$. Then, $x^{-1} \in S$, which implies there exists $r_0, \ldots, r_{n-1} \in R$ such that

$$\begin{aligned}&\implies r_0 + \cdots r_{n-1}x^{-n+1} + x^{-n} = 0\\ &\implies r_0x^{n-1} + \cdots + r_{n-1} + x^{-1} = 0\\ &\implies x^{-1} \in R.\end{aligned}$$

Problem 9. Suppose that S is an integral extension of R, and that I is an ideal of S. Show that I is a maximal ideal of S if and only if $I \cap R$ is a maximal ideal of R.

Solution 9. We consider the injective homomorphism $f : R/(I \cap R) \to S/I$, defined by $f(x + I \cap R) = x + I$. Since S is an integral extension of R, S/I is an integral extension of $\mathrm{im}(f)$. By **Problem 8**, we note S/I is a field if and only if $R/(I \cap R)$ is a field. The desired result then follows.

Problem 10. Let R be an integral domain. Show that R is the intersection of its localizations at all prime ideals $R_{\mathfrak{p}}$, and in fact is the intersection of its localizations at all maximal ideals $R_{\mathfrak{m}}$.

Solution 10. It suffices to prove the result for maximal ideals. The first inclusion is given to us for free: $R \subseteq S^{-1}R$ for any multiplicative set S. For the reverse inclusion, consider an element $\alpha \in \mathrm{Frac}(R)$ not in R. Consider the proper ideal of R $I_\alpha = \{r \in R |\ r\alpha \in R\}$. As I_α is proper, there exists maximal $\mathfrak{m} \supseteq I_\alpha$. We note $R_{\mathfrak{m}}$ does not contain α as that would imply there exists $r \notin \mathfrak{m}$ such that $r\alpha \in R$.

Problem 11. Prove that the following are equivalent for an integral domain R:

(1) R is integrally closed.
(2) $R_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p}$ of R.
(3) $R_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$ of R.

Solution 11. It suffices to show (1) $\iff$ (3) and (1) $\implies$ (2). (1) $\implies$ (3) and (1) $\implies$ (2) by Lemma 0.1.30. For (3) $\implies$ (1), we note that **Problem 10** tells us that

$$R = \bigcup_{\mathfrak{m}} R_{\mathfrak{m}}.$$

With this, we note that if $\alpha \in \mathrm{Frac}(R)$ is integral over R, α is integral over $R_{\mathfrak{m}}$ for all $\mathfrak{m}$. Then, since they're all integrally closed, $x \in R$.

CHAPTER 3.7

Projective Varieties

Problem 1. Write down the line through the points $(1:2:3)$ and $(2:3:5)$ in $\mathbb{P}^2$ as a vanishing set of some homogeneous ideal. Write down the line through the points $(1:2:4:8)$ and $(1:3:9:27)$ in $\mathbb{P}^3$.

Solution 1. Consider the plane f passing through $(1:2:3)$, $(2:3:5)$, and $(0:0:0)$, i.e. $V(f)$ where $f(x,y,z) = x+y-z$. Similarly, consider the plane g passing through $(1:2:3)$, $(2:3:5)$, and $(1:1:1)$: $V(g)$ where $g(x,y,z) = 2y-z-1$. Then, the line $V(f,g)$ passes through $(1:2:3)$ and $(2:3:5)$. We apply a similar argument for the 4 dimensional case. Let

$$\begin{aligned} f(x,y,z,w) &= -36x+24y-z-w \\ g(x,y,z,w) &= 42x-29y+2z+w \\ h(x,y,z,w) &= 66x-43y+z+2w. \end{aligned}$$

Then, $V(f,g,h)$ is our desired line.

Problem 2. In $\mathbb{P}^2$, for $0 \le i \le 2$, let $U_i = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 |\ x_i \neq 0\}$. Then U_i is isomorphic to $\mathbb{A}^2$; let us write $(x_{1/0}, x_{2/0})$ for the coordinates on U_0 via $(1 : x_1 : x_2) \mapsto (x_1, x_2)$ or more generally $(x_0 : x_1 : x_2) \mapsto (x_1/x_0, x_2/x_0)$. On $U_0 \cap U_1$, describe the coordinates $(x_{1/0}, x_{2/0})$ in terms of the coordinates $(x_{0/1}, x_{2/1})$.

Solution 2. $(1, x_{2/1})$.

Problem 3. Describe all homogeneous polynomials in x, y, z whose dehomogenization is x^2+y^3-1. Is there a preferred one?

Solution 3. Such polynomials are of the form $x^2z^n + y^3z^{n-1} - z^{n+2}$, for $n \in \mathbb{N}$. Setting $n=1$, we obtain the minimal (or *preferred*) homogeneous polynomial $x^2z + y^3z - z^3$.

Problem 4. Find all rational points on the projective varieties $V(x, xyz^3 - y^3z^2 + y^5) \subset \mathbb{P}^2$ and $V(z^2 + y^2 - 9x^2) \subset \mathbb{P}^2$.

Solution 4. For the first, we note $x = 0$, and, hence, $xyz^3 - y^3z^2 + y^5 = y^3(y-z)(y+z) = 0$. Our solutions are then $(0:0:1)$, $(0:1:1)$, and $(0:1:-1)$. For the second, we note

$$z^2 + y^2 - 9x^2 = 0 \iff \left(\frac{z}{3x}\right)^2 + \left(\frac{y}{3x}\right)^2 = 1.$$

As x is non-zero, we set $x = 1$. Then, using the parameterization of the unit circle, our rational solutions become

$$\left(1 : \frac{6t}{1+t^2} : \frac{3-3t^2}{1+t^2}\right).$$

Problem 5. Compute the Hilbert functions and Hilbert polynomials of the following projective varieties:

(1) $V(xy(x+y)) \subset \mathbb{P}^1$
(2) $V(x^2) \subset \mathbb{P}^2$
(3) $V(yz - x^2) \subset \mathbb{P}^2$
(4) $V(y^2z - x^3) \subset \mathbb{P}^2$
(5) $V(y^2 - x^2(x+z)) \subset \mathbb{P}^2$

Solution 5.

(1) We hope to show the monomial basis of $\mathcal{O}(V(xy(x+y)))_i$ is simply x^i, y^i, xy^{i-1}. We begin by noting $xy^2 = -x^2y$. Then, $x^a y^b = -x^{a-1}y^{b+1}$ with $a > 1$ and $b > 0$. Hence, the power of x in our monomial basis can only be 1 when y has a power greater 0. The desired result follows.
(2) As $x^2 = 0$, we note the highest power of x in our monomial basis can be 1. Thus, applying a stars and bars argument, we conclude the dimension of $\mathcal{O}(V(x^2))_i$ is
$$\binom{1+i}{i} + \binom{i}{1} = 2i + 1.$$
(3) By essentially the same argument, we conclude the dimension of $\mathcal{O}(V(x^2))_i$ is
$$\binom{1+i}{i} + \binom{i}{1} = 2i + 1.$$
(4) We note that the power of x in our monomial basis must be less than 3. Hence,
$$h_{\mathcal{O}(V(x^2))}(i) = \begin{cases} 2i+1 & i = 1 \\ 3i & i > 1 \end{cases}.$$
(5) As $y^2 = x^2(x+z)$, we note the dimension of $\mathcal{O}(V(y^2 - x^2(x+z)))_i$ is
$$\binom{1+i}{i} + \binom{i}{1} = 2i + 1.$$

Problem 6. Show that for any two lines L_1 and L_2 in $\mathbb{P}^2$, there is a projective transformation taking L_1 to L_2.

Solution 6. As a point is uniquely determined by two points, lets say L_1 is the line passing through $(a : b : c)$ and $p : q : r$ and L_2 is the line passing through $(a' : b' : c')$ and $p' : q' : r'$. We define a the map f_i such that
$$f_1(x, y, z) = \frac{p' - p}{a' - a}(x - a) + p'$$
$$f_2(x, y, z) = \frac{q' - q}{b' - b}(x - b) + q'$$
$$f_3(x, y, z) = \frac{r' - r}{c' - c}(x - c) + r'.$$
Then, define $f : L_1 \to L_2$ such that $f(x : y : z) = (f_1(x, y, z) : f_2(x, y, z) : f_3(x, y, z))$.

Problem 7. Let $\phi : \mathbb{P}^n \times \mathbb{P}^n \to \mathbb{P}^{n^2+2n}$ be the Segre embedding. Let $\Delta \subset \mathbb{P}^n \times \mathbb{P}^n$ be the diagonal, i.e. $\{(a, a) |\ a \in \mathbb{P}^n\}$. Show that $\phi(\Delta)$ is the 2-uple Veronese variety.

Solution 7. Notice that the image of an element in the diagonal is
$$\phi((x_0 : \cdots : x_n)(x_0 : \cdots : x_n))) = (x_0x_0 : x_0x_1 : \cdots : x_nx_n),$$
which contains coordinates who are precisely all monic polynomials in $x_0, \ldots, x_n$ of degree 2. The desired result follows.

Bibliography

[Con14] Keith Conrad. Separability. 2014.
[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.
[Lan02] Serge Lang. *Graduate Texts in Mathematics: Algebra*. Springer, 2002.
[RS] Simon Rubinstein-Salzedo. *Abstract Algebra*.