Math 71: Abstract Algebra

Prishita Dharampal

Credit Statement: Talked to Sair Shaikh'26, and Math Stack Exchange.

Problem 1. An element $e \in R$ is called an idempotent if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.

Solution.

1. Re is a two-sided ideal.
   A two-sided ideal is an abelian subgroup under addition and closed under multiplication.

   (a) Showing that Re is an abelian subgroup:

   $$Re = \{r_1e + r_2e + \cdots + r_ne \mid \forall r_i \in R,\, n \in \mathbb{Z}^+\}$$

   Using the distributive law:

   $$Re = \{(r_1 + r_2 + \cdots + r_n)e \mid \forall r_i \in R,\, n \in \mathbb{Z}^+\}$$

   And $(R, +)$ is an abelian group.

   (b) Showing that Re is closed under multiplication:
   Let $r \in R$, $r_ie \in R$,

   i. $r(r_ie) = (rr_i)e$, and by definition $rr_ie \in Re$.
   ii. $(r_ie)r = (r_ir)e$, again, by definition $r_ire \in Re$.
   iii. $r_1e \cdot r_2e = r_1r_2e^2 = r_1r_2e \in Re$, $\forall r_1e, r_2e \in Re$.

   Hence, Re a two-sided ideal.

2. e is an identity for Re.
   $\forall re \in Re$, $re.e = re^2 = re$, and $ere = re^2 = re$. Hence, the element is unchanged under multiplication by e, i.e., e is an identity.

3. $R(1-e)$ is a two-sided ideal.
   A two-sided ideal is an abelian subgroup under addition and closed under multiplication.

   (a) Showing that $R(1-e_)$ is an abelian subgroup:

   $$R(1-e) = \{r_1(1-e) + r_2(1-e) + \cdots + r_n(1-e) \mid \forall r_i \in R,\, n \in \mathbb{Z}^+\}$$

   But, using the distributive law:

   $$Re = \{(r_1 + r_2 + \cdots + r_n)(1-e) \mid \forall r_i \in R,\, n \in \mathbb{Z}^+\}$$

   And $(R, +)$ is an abelian group.

   (b) Showing that $R(1-e)$ is closed under multiplication:
   Let $r \in R$, $r_i(1-e) \in R$,

   i. $r(r_i(1-e)) = (rr_i)(1-e)$, and by definition $rr_i(1-e) \in R(1-e)$.
   ii. $(r_i(1-e))r = (r_i - r_ie)r = r_ir - r_ire = r_ir(1-e)$, again, by definition $r_ir(1-e) \in R(1-e)$.
   iii. $r_1(1-e), r_2(1-e) \in R(1-e)$

   $$\begin{aligned} r_1(1-e) \cdot r_2(1-e) &= (r_1 - r_1e)(r_2 - r_2e) \\ &= r_1r_2 - r_1r_2e - r_1er_2 + r_1r_2e^2 \\ &= r_1r_2 - r_1r_2e - r_1r_2e + r_1r_2e \\ &= r_1r_2(1-e) \in Re \end{aligned}$$

   Hence, $R(1-e)$ a two-sided ideal.

4. $(1-e)$ is an identity for $R(1-e)$.
   We note the following,

   $$(1-e)^2 = 1 - e - e + e = 1 - e \qquad (1-e)r = r - er = r - re = r(1-e)$$

   Then $\forall r(1-e) \in R(1-e)$, $r(1-e).(1-e) = r(1-e)$, and $(1-e)r(1-e) = r(1-e)^2 = r(1-e)$. Hence, the element is unchanged under multiplication by $(1-e)$, i.e., $(1-e)$ is an identity.

5. $R \cong Re \times R(1-e)$
   We can see that the ideals $(e), (1-e)$ are comaximal

   $$(e) + (1-e) = (e + 1 - e) = (1) = R$$

   Then, by the Chinese Remainder Theorem,

   $$R/(Re \cap R(1-e)) \cong R/Re \times R/R(1-e)$$

Claim: $Re \cap R(1-e) = 0$.
Assume $Re \cap R(1-e) \neq 0$, then there exists a non-zero $x \in Re \cap R(1-e)$. I.e $x = r_1 e = r_2 - r_2 e$ for some $r_1, r_2 \in R$. Then,

$$\begin{aligned} r_1 e &= r_2(1-e) \\ r_1 e^2 &= r_2(e-e^2) \\ r_1 e &= r_2(0) = 0 \end{aligned}$$

Hence, $x = 0$, which is a contradiction since we assumed x to be a non-zero element in the intersection.

Claim: $R/Re \cong R(1-e)$
Define the map $\varphi : R \to R(1-e)$, such that $r \to r(1-e)$. The kernel of this map $ker(\varphi) = \{a(1-e) = 0, \forall a \in R\}$.

$$a = a \cdot 1 = a \cdot (e + 1 - e) = ae + a(1-e) = ae$$

$\implies ker(\varphi) \subseteq Re$. For the reverse inclusion,

$$(re)(1-e) = re - re^2 = 0$$

$\implies Re \subseteq ker(\varphi) \implies Re = ker(\varphi)$.
By the First Isomorphism Theorem,

$$R/Re \cong R(1-e)$$

Claim: $R/R(1-e) \cong Re$
Define the map $\varphi : R \to Re$, such that $r \to re$. The kernel of this map $ker(\varphi) = \{ae = 0, \forall a \in R\}$.

$$a = a \cdot 1 = a \cdot (e + 1 - e) = ae + a(1-e) = a(1-e)$$

$\implies ker(\varphi) \subseteq R(1-e)$. For the reverse inclusion,

$$(r(1-e))e = re - re^2 = 0$$

$\implies R(1-e) \subseteq ker(\varphi) \implies R(1-e) = ker(\varphi)$.
By the First Isomorphism Theorem,

$$R/R(1-e) \cong Re$$

Then we can re-write

$$R/(Re \cap R(1-e)) \cong R/Re \times R/R(1-e)$$

as

$$R/\{0\} = R \cong R(1-e) \times Re$$

Hence proved.

Problem 2. Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

Solution.

Let K be an ideal in $R \times S$, where $K = \{(x, y)\}$. Then define I, J to be the ideals generated by all elements in K, where $y = 0$, and $x = 0$ respectively.

$$I = \{(x : (x, 0) \in K\} \qquad J = \{(y : (0, y) \in K\}$$

1. $K \subseteq I \times J$
   Let $(x, y) \in K$. Since an ideal is multiplicatively closed,

   $$(x, y)(1, 0) = (x, 0) \in K$$

   But $(x, 0) \in I$ (by definition of I). Similarly,

   $$(x, y)(0, 1) = (0, y) \in K$$

   But $(0, y) \in J$ (by definition of J). Then, $(x, y) \in I \times J$.

2. $I \times J \subseteq K$
   Let $(x, y) \in I \times J$, where x, y are generators. Then $(x, 0) \in K$, $(0, y) \in K$ (by definition). And since K is closed under addition $(x, 0) + (0, y) = (x, y) \in K$.

   Let $(x', y') \in I \times J$, where (x', y') are arbitrary elements. By definition x', y' are finite sums of the products of the generators of the ideal and the ring elements,

   $$x' = \sum_{i=1}^{n} r_i x_i \qquad y' = \sum_{i=1}^{n} s_i y_i$$

   Then we can represent $(x'y')$ as

   $$(x', y') = (r_1, 0)(x_1, 0) + \cdots + (r_n, 0)(x_n, 0) + (0, s_1)(0, y_1) + \cdots + (0, s_m)(0, y_m)$$

   I.e. $(x', y') \in K$.

Hence, $K = I \times J$. Since, K was an arbitrary ideal, this is true for any ideal of $R \times S$.

Problem 3. (A Public Key Code) Let N be a positive integer. Let M be an integer relatively prime to N and let d be an integer relatively prime to $\varphi(N)$, where φ denotes Euler's φ-function. Prove that if $M_1 \equiv M^d \pmod{N}$ then $M \equiv M_1^{d'} \pmod{N}$ where d' is the inverse of d modulo $\varphi(N)$; that is, $dd' \equiv 1 \pmod{\varphi(N)}$.

Remark. This result is the basis for a standard Public Key Code. Suppose $N = pq$ is the product of two distinct large primes (each on the order of 100 digits, for example). If M is a message, then $M_1 \equiv M^d \pmod{N}$ is a scrambled (encoded) version of M, which can be unscrambled (decoded) by computing $M_1^{d'} \pmod{N}$. These powers can be computed quite easily even for large values of M and N by successive squarings. The values of N and d (but not p and q) are made publicly known (hence the name), and then anyone with a message M can send their encoded message $M^d \pmod{N}$. To decode the message it seems necessary to determine d', which requires the determination of the value $\varphi(N) = \varphi(pq) = (p-1)(q-1)$ (no one has as yet proved that there is no other decoding scheme, however). The success of this method as a code rests on the necessity of determining the factorization of N into primes, for which no sufficiently efficient algorithm exists. For example, the most naive method of checking all factors up to $\sqrt{N}$ would here require on the order of 10^{100} computations, or approximately 300 years even at 10 billion computations per second, and of course one can always increase the size of p and q.

Problem 4. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals

$$I_2 = (2,\ 1+\sqrt{-5}), \qquad I_3 = (3,\ 2+\sqrt{-5}), \qquad I_3' = (3,\ 2-\sqrt{-5}).$$

(a) Prove that I_2, I_3, and I_3' are nonprincipal ideals in R.

(b) Prove that the product of two nonprincipal ideals can be principal by showing that I_2^2 is the principal ideal generated by 2, i.e. $I_2^2 = (2)$.

(c) Prove similarly that $I_2 I_3 = (1-\sqrt{-5})$ and $I_2 I_3' = (1+\sqrt{-5})$ are principal ideals. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$

Solution.

(a)

1. Assume I_2 is principal. Then there must be some element x that generates the whole ideal:
$$I_2 = (2, 1+\sqrt{-5}) = (x)$$
In particular, $x \mid 2$ and $x \mid (1+\sqrt{-5}) \implies N(x) \mid N(2)$ and $N(x) \mid N(1+\sqrt{-5})$. $N(2) = 4, N(1-\sqrt{-5}) = 6$, i.e $N(x) = 1$ or $N(x) = 2$. If $N(x) = 1$, then x is a unit and the ideal generated is the whole ring. Hence, a contradiction ($1 \notin I_2$). If $N(x) = 2$ then $x = a + b\sqrt{-5}$ such that $a^2 + 5b^2 = 2$, since $a^2, b^2 > 0$, there exist no integer solutions for this equation. I.e $N(x) \neq 2$. Since, neither of the solutions work I_2 is not principal.
2. Similarly, assume I_3 is principal. Then there exists some element x that generates the whole ideal:
$$I_3 = (3, 2+\sqrt{-5}) = (x)$$
In particular, $x \mid 3$ and $x \mid (2+\sqrt{-5}) \implies N(x) \mid N(3)$ and $N(x) \mid N(2+\sqrt{-5})$. $N(3) = 9, N(2-\sqrt{-5}) = 9$, i.e $N(x) = 1$, $N(x) = 3$ $N(x) = 9$. If $N(x) = 1$, then x is a unit and the ideal generated is the whole ring. Hence, a contradiction ($1 \notin I_2$). If $N(x) = 3$ then $x = a + b\sqrt{-5}$ such that $a^2 + 5b^2 = 3$, since $a^2, b^2 > 0$, there exist no integer solutions for this equation. $\implies N(x) \neq 3$. If $N(x) = 9$ then $x = a + b\sqrt{-5}$ such that $a^2 + 5b^2 = 9$. There are two integer solutions:
   i. $a = 3, b = 0$ Then $I_3 = (3)$, which is not true because $2 + \sqrt{-5} \notin (3)$.
   ii. $a = \pm 2, b = \pm 1$. Then $I_3 = (\pm 2 \pm \sqrt{-5})$, which is not true because $3 \notin (\pm 2 \pm \sqrt{-5})$ (Since $3/(\pm 2 \pm \sqrt{-5}) \notin R$).

   Since, neither of the solutions work I_3 is not principal.
3. The same argument holds for I_3' because $N(2+\sqrt{-5}) = N(2-\sqrt{-5})$.

(b) $I_2^2 = I_2 \cdot I_2 = (2\cdot 2, 2\cdot(1+\sqrt{-5}), (1+\sqrt{-5})\cdot(1+\sqrt{-5})) = (4,\ 2+2\sqrt{-5},\ 4+2\sqrt{-5})$. Since the ideal is an abelian group, $I = (a, b) \supseteq (a-b) \implies I_2^2 \supseteq (-2) = (2)$, And the

opposite containment is also true because $2 \mid 4$, $2 \mid (2+\sqrt{-5})$, $2 \mid (4+2\sqrt{-5})$. Hence, $I_2^2 = (2)$, and is principal.

(c) (i) $I_2 I_3 = (1-\sqrt{-5})$

$$\begin{aligned} I_2 I_3 &= (2\cdot 3, 2\cdot(2+\sqrt{-5}), (1+\sqrt{-5})\cdot 3, (1+\sqrt{-5})(2+\sqrt{-5}) \\ &= (6,\ 4+2\sqrt{-5},\ 3+3\sqrt{-5}, -3+3\sqrt{-5}) \end{aligned}$$

i. $6 = (1-\sqrt{-5})(1+\sqrt{-5})$
ii. $4+2\sqrt{-5} = (1-\sqrt{-5})(-1+\sqrt{-5})$
iii. $3+3\sqrt{-5} = (1-\sqrt{-5})(-1+2\sqrt{-5})$
iv. $-3+3\sqrt{-5} = (1-\sqrt{-5})(-3)$

Same as above, since the ideal is an abelian group, $I = (a,b) \supseteq (a-b) \implies I_2 I_3 \supseteq (1-\sqrt{-5})$, And the opposite containment is also true because $(1-\sqrt{-5})$ divides all the generators. Hence, $I_2 I_3 = (1-\sqrt{-5})$, and is principal.

(ii) $I_2 I_3' = (1+\sqrt{-5})$

$$\begin{aligned} I_2 I_3' &= (2\cdot 3, 2\cdot(2-\sqrt{-5}), (1+\sqrt{-5})\cdot 3, (1+\sqrt{-5})(2-\sqrt{-5}) \\ &= (6,\ 4-2\sqrt{-5},\ 3+3\sqrt{-5}, 7+\sqrt{-5}) \end{aligned}$$

i. $6 = (1+\sqrt{-5})(1-\sqrt{-5})$
ii. $4-2\sqrt{-5} = (1+\sqrt{-5})(-3-\sqrt{-5})$
iii. $3+3\sqrt{-5} = (1+\sqrt{-5})(3)$
iv. $7+\sqrt{-5} = (1-\sqrt{-5})(2-\sqrt{-5})$

Same as above, since the ideal is an abelian group, $I = (a,b) \supseteq (a-b) \implies I_2 I_3' \supseteq (1+\sqrt{-5})$, And the opposite containment is also true because $(1+\sqrt{-5})$ divides all the generators. Hence, $I_2 I_3' = (1+\sqrt{-5})$, and is principal.

(iii) Since $\mathbb{Z}[\sqrt{-5}]$ is commutative $I_2^2 I_3 I_3' = I_2 I_3 I_2 I_3'$ and we know that

$$I_2 I_3 = (1-\sqrt{-5}) \quad \text{and} \quad I_2 I_3' = (1+\sqrt{-5})$$

then $I_2 I_3 I_2 I_3' = ((1-\sqrt{-5})(1+\sqrt{-5})) = (6)$.

Problem 5. Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.

Solution.

We know that an ideal P is prime in a ring R if R/P is an integral domain, and the ideal is maximal if R/P is a field.

1. Consider the homomorphism $\varphi : \mathbb{Z}[x, y] \to \mathbb{Z}$ such that $\varphi(ax + by + c) = c$. It's kernel is all polynomials with zero constant term, i.e, precisely the ideal (x, y).

   $$\mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}$$

   Since, $\mathbb{Z}$ is an integral domain, (x, y). However, because $\mathbb{Z}$ is not a field, (x, y) is not maximal.

2. Consider the homomorphism $\varphi : \mathbb{Z}[x, y] \to \mathbb{Z}/2\mathbb{Z}$ such that $\varphi(ax + by + c) = c \pmod 2$. It's kernel is all polynomials with even constant term, i.e, precisely the ideal $(2, x, y)$.

   $$\mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}/2\mathbb{Z}$$

   Since, $\mathbb{Z}/2\mathbb{Z}$ is field, $(2, x, y)$ is maximal and thus also prime.

Problem 6.
Call a positive integer n *special* if there exists an integer m with $1 < m < n$ such that

$$1 + 2 + \cdots + (m-1) \;=\; (m+1) + \cdots + n.$$

For example, $n = 8$ is special with $m = 6$, while $n = 7$ is not special. Find all positive integers that are special. **Hint.** Relate the pairs (n, m) to integer solutions of $a^2 - 2b^2 = 1$, i.e. units in $\mathbb{Z}[\sqrt{2}]$ of norm 1. You can use the book's description of the units in $\mathbb{Z}[\sqrt{2}]$.

Solution.

Using the formula $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ we get:

$$\frac{(m-1)m}{2} = \frac{n(n+1)}{2} - \frac{m(m+1)}{2} \implies n^2 + n - 2m^2 = 0$$

Completing the square:

$$\begin{aligned} n^2 + n - 2m^2 &= 0 \\ n^2 + n - \frac{1}{4} + \frac{1}{4} - 2m^2 &= 0 \\ \left(n + \frac{1}{2}\right)^2 - 2m^2 &= \frac{1}{4} \\ (2n+1)^2 - 2(2m)^2 &= 1 \end{aligned}$$

Let $a = 2n + 1$, $b = 2m$, then the equation looks like $a^2 - 2b^2 = 1$.
For any $\alpha = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, the norm looks like $(x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2$. Hence, (a, b) are units (with norm $+1$) in $\mathbb{Z}[\sqrt{2}]$. We know that the full group of units of $\mathbb{Z}[\sqrt{2}] = \{\pm(1 + \sqrt{2})^n | n \in \mathbb{Z}\}$ (Pg. 230). The norm for the positive case, $(1 + \sqrt{2})^n$ is -1, and the norm for the negative case, $(-1 - \sqrt{2})^n$ is 1. Hence, $(-1 - \sqrt{2})^n, n \in \mathbb{Z}$ are all solutions to our equation.

Problem 7.
Prove the following presentations:

(a) $A_4 = \langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$

(b) $S_4 = \langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \rangle$

(c) $A_5 = \langle x, y \mid x^2 = y^3 = (xy)^5 = 1 \rangle$

Solution.

(a) Consider the subgroup $H = \langle (12)(34), (123) \rangle \in A_4$. There are at least 7 distinct elements in this subgroup ($\{1, a, b, ab, ba, b^2, ab^2\}, a = (12)(34), b = (123)$) by Lagrange's Theorem, $H = A_4$. ($H \neq S_4$ because we cannot get a 4-cycle by multiplying a 2-2-cycle and a 3-cycle). Next, let G be the group with the presentation $\langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$. Then we can define a map $\varphi : G \to A_4$, which maps $x \to (12)(34)$, $y \to (123)$.

(a) $x^2 = (12)(34)(12)(34) = (12)^2(34)^2 = 1$.

(b) $y^3 = (123)^3 = 1$.

(c) $(xy)^3 = ((12)(34)(123))^3 = ((1)(243))^3 = (243)^3 = 1$

Since, the generators map to the generators and all of the relations hold, φ is an isomorphism. I.e. $A_4 = \langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$ is a valid presentation.

(b) We know that $S_n = \langle (12), (12 \cdots n) \rangle \implies S_4 = \langle (12)(1234) \rangle$. Also note, $(12)(234) = (2341) = (1234)$, ie, we can write $S_4 = \langle (12), (234) \rangle$

Next, let G be the group with the presentation $\langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \rangle$. Then we can define a map $\varphi : G \to S_4$, which maps $x \to (12)$, $y \to (234)$. Then we check the relations:

(a) $x^2 = (12)^2 = 1$.

(b) $y^3 = (234)^3 = 1$.

(c) $(xy)^4 = ((12)(234))^4 = (1243)^4 = 1$

Since, the generators map to the generators and all of the relations hold, φ is an isomorphism. I.e. $S_4 = \langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \rangle$ is a valid presentation.

(c) Consider the subgroup $H = \langle (12)(34), (135) \rangle \leq A_5$. $(12)(34)(135) = (14352)$, and $(135)(12)(34) = (12345)$.

Let G be the group with the presentation $\langle x, y \mid x^2 = y^3 = (xy)^5 = 1 \rangle$. Then we can define a map $\varphi : G \to H$, which maps $x \to (12)(34)$, $y \to (135)$.

(a) $x^2 = (12)(34)(12)(34) = (12)^2(34)^2 = 1$.

(b) $y^3 = (135)^3 = 1$.

(c) $(xy)^5 = ((12)(34)(135))^5 = (14352)^5 = 1$

Then, φ is a homomorphism. Since, the generators map to the generators and all of the relations hold, φ is an isomorphism.

From the presentation, we know that G contains an elements of order $2, 3, 5$. By Cauchy's Theorem, we know that the order of G is at least 30. Since, $G \leq A_5 \implies |G| \mid 60$. If $|G| = 30 \implies [A_5 : G] = 2$, implying that A_5 has normal subgroup, but A_5 is simple, hence, $|G| \neq 30$. Then, the subgroup G must equal A_5.

Problem 8.
For a field F, denote by $\mathrm{PGL}_2(F)$ and $\mathrm{PSL}_2(F)$ the quotients of $\mathrm{GL}_2(F)$ and $\mathrm{SL}_2(F)$ by their respective normal subgroups consisting of the nonzero scalar matrices of the identity.

(a) Prove that for any field F, the kernel of the action of $\mathrm{GL}_2(F)$ on the set of lines through the origin in F^2 is exactly the subgroup of nonzero scalar matrices. Deduce that the induced action of $\mathrm{PGL}_2(F)$ on the set of lines is faithful.

(b) Prove that if F_q is a finite field with q elements, then the number of lines through the origin in the vector space F_q^2 is $q+1$.

(c) Recall, from Problem Set #2, the construction of the field F_4 of order 4. Prove that

$$\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{SL}_2(\mathbb{F}_4) \cong A_5$$

Hint. Consider the action on the set of lines through the origin in $\mathbb{F}_4^2$.

(d) Prove that $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ and that $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$. **Hint.** The action on the set of lines through the origin in the vector space $\mathbb{F}_5^2$ gives an injective homomorphism $\mathrm{PGL}_2(\mathbb{F}_5) \to S_6$. Count the number of $(2,2,2)$-cycles in S_6 not in the image, then let $\mathrm{PGL}_2(\mathbb{F}_5)$ act on them by conjugation to obtain a new permutation representation.

Solution.

(a) Let X be the set of lines passing through the origin in F^2. We can represent an element in this set (a line) as $a + \lambda b$, where a, b are points on the line and $\lambda \in F$. Since, the lines pass through the origin $a = 0$, and $b = \begin{pmatrix} p \\ q \end{pmatrix}$. Then let $\vec{v} \in X, \vec{v} = \begin{pmatrix} \lambda p \\ \lambda q \end{pmatrix}$

The action of $GL_2(F)$ on the set of lines through the origin in F^2, X, looks like $\varphi : GL_2(F) \times X \to X$. The kernel of this action $ker(\varphi)$ are elements in $GL_2(F)$ that fix all elements of X. (Note: fixing a line through the origin means it only scalar multiplies each vector.)

Let $K \in ker(\varphi)$, then $K = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}$, such that $Kx = \alpha\vec{v}$, for some α. Then consider the basis vectors:

(a) $\vec{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $K\vec{v} = \alpha\vec{v} \implies \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_3 \end{pmatrix} \implies k_3 = 0$

(b) $\vec{v} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $K\vec{v} = \alpha\vec{v} \implies \begin{pmatrix} k_1 & k_2 \\ 0 & k_4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} k_2 \\ k_4 \end{pmatrix} \implies k_2 = 0$

(c) $\vec{v} = \begin{pmatrix}1\\1\end{pmatrix}$, $K\vec{v} = \alpha\vec{v} \implies \begin{pmatrix}k_1 & 0\\0 & k_4\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}k_1\\k_4\end{pmatrix} \implies \begin{pmatrix}k_1\\k_4\end{pmatrix} = \alpha\begin{pmatrix}1\\1\end{pmatrix}$

$\implies k_1 = k_4$

I.e. any matrix $K \in ker(\varphi)$ is a scalar matrix; $ker(\varphi) \subseteq$ Set of Scalar Matrices. To show equality, we must show opposite containment: Set of Scalar Matrices $\subseteq ker(\varphi)$

Let A be a scalar matrix, then

$$A = \begin{pmatrix}a & 0\\0 & a\end{pmatrix} \implies A\vec{v} = \begin{pmatrix}a & 0\\0 & a\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} \implies \begin{pmatrix}ax\\ay\end{pmatrix} \implies a\begin{pmatrix}x\\y\end{pmatrix} \implies A \in ker(\varphi)$$

Since A was an arbitrary scalar matrix, we can say that the
Set of Scalar Matrices $\subseteq ker(\varphi) \implies$ Set of Scalar Matrices $= ker(\varphi)$.

By the First Isomorphism Theorem,

$$GL_2(F)/ker(\varphi) \cong im(\varphi)$$

Since, $PGL_2(F)$ is the quotient of $GL_2(F)$ by it's normal subgroup consisting of non-zero scalar matrices, we can re-write the above equation as,

$$GL_2(F)/ker(\varphi) = PGL_2(F) \cong im(\varphi)$$

I.e the kernel of the induced action of $PGL_2(F)$ on X is trivial, hence the action is faithful.

(b) A line in F_q^2 can be represented as $a + \lambda b$, where a, b are two points on the line, and $\lambda \in F_q$. If the line passes through the origin, we know that one of the points is $(0,0) \implies p = 0$. That is, all lines passing through the origin in F_q^2 can be represented as λb. Since all lines intersect at $(0,0)$ we know that a given line has $(q-1)$ unique points.

There are q^2 points in F_q^2. Excluding $(0,0)$, there are $q^2 - 1$ points. Then we can determine the number of unique lines through the origin in F_q^2 by $(q^2-1)/(q-1) = q+1$. Hence proved.

(c) From Problem Set 2, $\mathbb{F}_4 = \{0, 1, x, y \mid x^2 = y, y^2 = x, 1 + x = y, 1 + y = x\}$

(i) $PSL_2(\mathbb{F}_4) \cong A_5$
We know that the order of $GL_2(F_q) = (q^2-1)(q^2-q)$, where F_q is a finite field. Order of $GL_2(\mathbb{F}_4) = 180$. Using part (a), the kernel of the action of $GL_2(\mathbb{F}_4)$ on the set of lines through the origin in $\mathbb{F}_4^2$ is the subgroup of nonzero scalar matrices, $ker = \{\lambda I, \lambda \in \mathbb{F}_4^\times\} \implies |ker| = 3$.
$GL_2(\mathbb{F}_4)/ker \cong PGL_2(\mathbb{F}_4)$ (by definition of $PGL_2(F)$).
$|PGL_2(\mathbb{F}_4)| = |GL_2(\mathbb{F}_4)|/3 = 60$.

Consider the action of $PGL_2(\mathbb{F}_4)$ on the set of all lines through the origin in $\mathbb{F}_4^2$. From part (b), we know that $\mathbb{F}_4^2$ has 5 lines. We then define a homomorphism $\varphi : PGL_2(\mathbb{F}_4) \to S_5$ with trivial kernel (the action is faithful, part(a)).

By the First Isomorphism Theorem, $PGL_2(\mathbb{F}_4)$ is isomorphic to a subgroup of S_5 of order 60. Since A_5 is the only one subgroup of S_5 of order 60, we can say $PSL_2(\mathbb{F}_4) \cong A_5$.

(ii) $PSL_2(\mathbb{F}_4) \cong SL_2(\mathbb{F}_4)$

$PSL_2(\mathbb{F}_4)$ by definition is the the quotient of $SL_2(\mathbb{F}_4)$ by it's normal subgroup consisting of the non-zero scalar matrices of the identity.

$det(\lambda I) = \lambda^2 det(I)$, 0^2, x^2, $y^2 \neq 1 \implies \lambda = 1$

The only non-zero scalar matrix in $SL_2(\mathbb{F}_4)$ is the identity matrix. Then the normal group that $SL_2(\mathbb{F}_4)$ will be quotiented by is the trivial subgroup.

$$SL_2(\mathbb{F}_4)/\{I\} \cong SL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4)$$

(iii) $PGL_2(\mathbb{F}_4) \cong PSL_2(\mathbb{F}_4)$

$PGL_2(\mathbb{F}_4)$ is defined as $GL_2(\mathbb{F}_4)/\langle \lambda I \rangle$. Let $[A]$ be a coset in $PGL_2(\mathbb{F}_4)$, $[A] = A\lambda I$.

$$det(A\lambda I) = det(A) \cdot det(\lambda I) = det(A) \cdot \lambda^2$$

Let the representative of the equivalence class $[A]$ be $A\lambda$, where $\lambda = \sqrt{\frac{1}{det(A)}}$, since every element has a square root in $\mathbb{F}_4$. Then the determinant of $[A], \forall [A] \in PGL_2(\mathbb{F}_4)$ is 1. Then we can define a homomorphism $\varphi : PGL_2(\mathbb{F}_4) \to PSL_2(\mathbb{F}_4)$, mapping $[A]$ to the corresponding matrix in $PSL_2(\mathbb{F}_4)$. The kernel of this homomorphism $ker(\varphi) = \{\lambda I = I\} \implies \lambda = 1$. Hence, the kernel is trivial.

The order of $SL_2(F_q) = q^3 - q \implies SL_2(\mathbb{F}_4) = 60 \implies PSL_2(\mathbb{F}_4) = 60$. Also from part (i), we know that the order of $PSL_2(\mathbb{F}_4)$ is 60. Hence, we can say that φ is an isomorphism, $PGL_2(\mathbb{F}_4) \cong PSL_2(\mathbb{F}_4)$.

$$PGL_2(\mathbb{F}_4) \cong PSL_2(\mathbb{F}_4) \cong SL_2(\mathbb{F}_4) \cong A_5$$

Problem 9.
Some linear algebra over the field of order 9.

(a) Prove that $\mathbb{F}_3[i] = \{0, \pm 1, \pm i, \pm 1 \pm i\}$, where $i^2 = -1$ and all other arithmetic is done modulo 3, is a field of order 9, which we call $\mathbb{F}_9$.

(b) Prove that $\mathrm{PGL}_2(\mathbb{F}_9)$ is not isomorphic to S_6, even though they have the same order. **Hint.** Use linear algebra to bound the sizes of certain conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_9)$ and compare to what is known in S_6.

(c) Prove, on the other hand, that $\mathrm{PSL}_2(\mathbb{F}_9) \cong A_6$.
Hint. Find a subgroup of $\mathrm{PSL}_2(\mathbb{F}_9)$ isomorphic to A_5, then let it act on its 6 cosets to obtain a permutation representation.

Solution.

(a) Consider the Euclidean Domain $\mathbb{Z}[i]$, and the ideal generated by $3, (3)$. We know that all EDs are PIDs (Proposition 1, Chapter 8). Then to show that (3) is maximal we only need to prove that it is prime. Assume 3 is not irreducible, i.e.

$$\exists a+bi, c+di \in \mathbb{Z}[i] : (a+bi)(c+di) = 3 \implies N(a+bi)N(c+di) = N(3) = 9 = (a^2+b^2)(c^2+d^2)$$

Then, wlog, the possible values for a^2+b^2, c^2+d^2 are: $1, 9$ or $3, 3$. WLOG, we can see that $a^2 + b^2 \neq 3, a, b \in \mathbb{Z}$. However, if $a^2 + b^2 = 1$, then $a + bi$ is a unit. Thus, a contradiction.

3 is prime in $\mathbb{Z}[i]$, and hence the ideal generated by 3 is maximal.

We know that the quotient of a ring by a maximal ideal is a field. An element in the quotient $\mathbb{Z}[i]/(3)$ looks like $a + bi$ where $a, b \in \mathbb{Z}/3\mathbb{Z}$. That is,

$$\begin{aligned}\mathbb{Z}[i]/(3) &= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\} \\ &= \{0, 1, -1, i, -i, 1+i, 1-i, -1+i, -1-i\}, \quad 2 \equiv -1 \pmod 3 \\ &= \{0, \pm 1, \pm i, \pm 1 \pm i\}\end{aligned}$$

where $i^2 = -1$. Then we can say that $\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[i]$. Also, by counting, we can see $|\ \mathbb{F}_3[i]\ | = 9$.

Hence, $F_3[i]$ is a field of order 9, where arithmetic is done modulo 3 and $i^2 = -1$.