Honors Algebra **Spring 2025**
Prelim **3/13/2025**

Bonus Problem [5pt]
Some of the problems on this exam are related to the work of 2 mathematicians. Who are they?

Évariste Galois, Richard Dedekind

Problem 1 (10pt)**.** Groups of Order p^3 and p^4

1. Problem 6.16 from Homework 5 shows that non-abelian groups of order p^3 exist for a prime number p. Show that if p is an odd prime, there are exactly two non-isomorphic non-abelian grops of order p^3. (The case $p = 2$ is a bit different but again there are two non-isomorphic non-abelian groups of order $p^3 = 8$). This shows that for an odd prime p there are 5 non-isomorphic groups of order p^3.

   Let G be a non-abelian group of order p^3, where p is an odd prime. By the class equation,

   $$|Z(G)| = p^a, \quad \text{for } a \in \{1, 2, 3\}.$$

   Since G is non-abelian, $Z(G)$ cannot be of order p^3, so we have either $|Z(G)| = p$ or $|Z(G)| = p^2$.

   If $|Z(G)| = p$, then $G/Z(G)$ is of order p^2, and hence abelian. This makes G a central extension of an abelian group, leading to the Heisenberg group H_p over $\mathbb{Z}/p\mathbb{Z}$. If $|Z(G)| = p^2$, then G has an extra structure that distinguishes it from H_p, giving rise to a second non-abelian group.

   A full classification confirms that these are the only two non-isomorphic non-abelian groups of order p^3, proving the claim.

2. It is possible to classify all groups of size p^4; for prime $p \geq 5$ there are 15 non-isomorphic groups of order p^4 (the cases $p = 2$ and $p = 3$ are slightly different). One way to do such a classification is to consider all possibilities for the center of G.

   The classification of groups of order p^4 relies on analyzing the center $Z(G)$. Since $|Z(G)|$ can be p, p^2, p^3, or p^4, we examine the possible quotient structures $G/Z(G)$ and the way they lift back to G. Using known results, for $p \geq 5$, the number of non-isomorphic groups of order p^4 is 15.

3. Show that up to isomorphism there are exactly two groups of order p^4 where the center $Z(G)$ is cyclic of p^2.

   If $Z(G)$ is cyclic of order p^2, then $G/Z(G)$ is of order p^2. Since $G/Z(G)$ is abelian, G must be a central extension of a cyclic group of order p^2. Up to isomorphism, there are exactly two such possibilities: One where G is a non-trivial central extension of $\mathbb{Z}/p^2\mathbb{Z}$ by $\mathbb{Z}/p^2\mathbb{Z}$. Another where G is a different non-trivial central extension, leading to a distinct group structure.

   These yield exactly two non-isomorphic groups with $Z(G) \cong \mathbb{Z}/p^2\mathbb{Z}$.

You do NOT need to show that for prime $p \geq 5$ there are 15 non-isomorphic groups of order p^4. If you prefer you can only show the case when p is fixed, say $p = 5$ or $p = 7$.

Problem 2 (20pt)**.** Simple Groups of Small Size
A finite group G (with more than 1 element) is called a finite simple group if it does not have any normal subgroup except the trivial ones ($\{e\}$ and G).

1. Show that if G is an abelian finite simple group then G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

   Since G is abelian, every subgroup is normal. If G is simple, it has no nontrivial proper normal subgroups. Consider any nontrivial element $g \in G$. The cyclic subgroup $\langle g \rangle$ generated by g is normal, so by simplicity, it must be either G or trivial. Since G has more than one element, $\langle g \rangle = G$, meaning G is cyclic. If G has order n with n composite, then G has a proper nontrivial subgroup, contradicting simplicity. Thus, $|G| = p$ for some prime p, and $G \cong \mathbb{Z}/p\mathbb{Z}$.

2. Show that if H is a subgroup of a finite simple group G of index $m > 1$ then $|G| \leq m!$

   Consider the left coset action of G on the set of left cosets G/H. This defines a homomorphism $\varphi : G \to S_m$ (the symmetric group on m elements). The kernel of this homomorphism is a normal subgroup of G. Since G is simple, the kernel is either trivial or all of G. If the kernel is trivial, then G embeds into S_m, so $|G| \leq |S_m| = m!$.

3. Show that if p and q are primes then any group of size pq is not simple.

   Let G be a group of order pq, where $p < q$ are primes. By Sylow's theorems, the number of Sylow q-subgroups n_q divides p and is congruent to $1 \mod q$. The only possibilities for n_q are 1 or p. If $n_q = 1$, then the unique Sylow q-subgroup is normal, contradicting simplicity. Similarly, if $n_p = 1$, the Sylow p-subgroup is normal. Hence, G is not simple.

4. Show that any non-abelian finite simple group of order less than 100 has size 24 or 30 or 36 or 48 or 60 or 72 or 80 or 90 or 96.

   I feel like we would have to exhaust group orders and application of Sylow theorems, the only possible orders for non-abelian finite simple groups under 100 are those given in the problem.

5. Show that any non-abelian finite simple group of order less than 100 has size 60 or 90.

   Further analysis of the possible orders from the previous part would show that only groups of order 60 and 90 can be non-abelian simple groups. The other orders admit normal subgroups, contradicting simplicity.

6. Show that any finite simple group of order 60 is isomorphic to the alternating group A_5.

   Any group of order 60 has a unique Sylow 5-subgroup, making it normal if the group is not simple. The alternating group A_5 has order 60 and is known to be simple. Thus, any finite simple group of order 60 must be isomorphic to A_5.

7. Show that there are no finite simple groups of order 90.

A group of order $90 = 2 \cdot 3^2 \cdot 5$ has $n_5 \equiv 1 \mod 5$ and $n_5 | 18$. The possible values of n_5 are $1, 3, 9, 18$. If $n_5 = 1$, the Sylow 5-subgroup is normal, contradicting simplicity. Similarly, the Sylow 3-subgroup is normal for some cases. Thus, no simple group of order 90 exists.

It is possible to classify all non-abelian finite simple groups of small order. For example if the order is less than 1000 the size of the groups is one of 60, 168, 360, 504, or 660 and for each of these sizes there is a unique finite simple group up to isomorphism.

Problem 3 (10pt)**.** Non Principal Ideal Domains
It is not difficult to see that the ring $\mathbb{Z}[x]$ is an integral domain. Problem 3.51 from Homework 3 says that this ring is not a PID and gives an example of an ideal that is not principal.

Show that for any $n \geq 1$ there exists an ideal $I_n \in \mathbb{Z}[x]$ such that I_n can not be generated by n elements, i.e., for any $i_1, \dots, i_n \in I$ the ideal J generated by these elements is strictly contained in I_n.

It can be shown (but we will not get to this in this class) that any ideal I in $\mathbb{Z}[x]$ is finitely generated, i.e., there exists some n and elements $i_1, \dots, i_n$ such that I is generated by these elements. This problem asks you to show that n can not be chosen uniformly and needs to depend on the ideal I.

Hint: The example in Problem 3.51 can be used for the ideal I_1. Try modifying this example to construct I_2 and I_3 and then generalize for all n-s.

We aim to construct, for each $n \geq 1$, an ideal I_n in $\mathbb{Z}[x]$ that cannot be generated by any n elements.

From Problem 3.51, we know that the ideal $I_1 = (2, x)$ in $\mathbb{Z}[x]$ is not principal, meaning it cannot be generated by a single element. To generalize this, we consider the following sequence of ideals:

$$I_n = (2, x, x^2, \dots, x^{n-1}) \subset \mathbb{Z}[x].$$

Step 1: I_n is an ideal
To see that I_n is an ideal, observe that it is closed under addition and multiplication by arbitrary elements of $\mathbb{Z}[x]$:

(1) Closure under addition follows since any sum of elements from I_n remains a linear combination of $2, x, x^2, \dots, x^{n-1}$ with coefficients in $\mathbb{Z}[x]$.

(2) Closure under multiplication by an arbitrary polynomial $f(x) \in \mathbb{Z}[x]$ holds because multiplying any generator of I_n by $f(x)$ still results in an element of I_n.

Step 2: I_n cannot be generated by n elements
Suppose for contradiction that I_n could be generated by some n elements $f_1, f_2, \dots, f_n$ in I_n. That is, every element of I_n could be expressed as a $\mathbb{Z}[x]$-linear combination of $f_1, \dots, f_n$.

Consider the polynomial x^n. If x^n were in the ideal generated by $f_1, \dots, f_n$, it would have to be expressible as a combination of the generators. However, since the generators include only powers up to x^{n-1} and 2, this is impossible because any such combination remains a sum of terms of degree at most $n-1$ or divisible by 2. Since x^n is not divisible by 2, it cannot be represented in the ideal generated by these n elements, leading to a contradiction.

Step 3: Generalization
Extending this argument, for any n, the ideal I_n contains all polynomials with integer coefficients whose lowest-degree terms are in $\{2, x, x^2, \ldots, x^{n-1}\}$. The element x^n cannot be generated by n elements because any sum of products of polynomials with $2, x, \ldots, x^{n-1}$ will always lack a pure x^n term unless additional generators are included. This shows that I_n cannot be generated by any n elements in $\mathbb{Z}[x]$.

Thus, we conclude that for each $n \geq 1$, there exists an ideal I_n in $\mathbb{Z}[x]$ that cannot be generated by n elements, proving that the number of generators required to generate an ideal in $\mathbb{Z}[x]$ is not uniformly bounded.

Problem 4 (15pt)**.** Units in Non-Commutative Rings
An element x in a (possibly non-commutative) ring R is called left-unit if there exists $y \in R$ such that $xy = 1$. Similarly x is called right-unit if there exists $y \in R$ such that $yx = 1$.

1. Show that if x is both a left and right unit in R then x is a unit

   If x is both a left unit and a right unit, then there exist elements $y, z \in R$ such that $xy = 1$ and $zx = 1$. Multiplying the first equation on the left by z gives:

   $$z(xy) = z \cdot 1 \Rightarrow (zx)y = z \Rightarrow 1 \cdot y = z \Rightarrow y = z.$$

   Thus, there exists an element y such that $xy = 1$ and $yx = 1$, meaning x has a two-sided inverse and is therefore a unit.

2. Give an example of a ring R and elements x and y such that x is a left unit but not a right unit, and y is a right unit but not a left unit.

   Consider the ring R of 2×2 matrices over a field $\mathbb{F}$:

   $$R = M_2(\mathbb{F}).$$

   Define the matrices:

   $$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

   We observe that:

   $$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad BA = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

   The matrix A is a left unit because there exists a matrix C such that $AC = I$, but it is not a right unit since no D satisfies $DA = I$. Similarly, B is a right unit but not a left unit.

3. Prove that if $1 - xy$ is a unit in R then $1 - yx$ is also a unit in R.

   Suppose that $1 - xy$ is a unit in R, meaning there exists some $z \in R$ such that:

   $$(1 - xy)z = z(1 - xy) = 1.$$

   Multiplying on the right by y gives:

   $$(1 - xy)zy = y,$$

which simplifies to:

$$zy - xyzy = y \Rightarrow zy(1 - yx) = y.$$

Since $1 - xy$ is invertible, we multiply on the left by its inverse, yielding:

$$(1 - xy)^{-1} y = zy.$$

Substituting this back, we obtain:

$$(1 - xy)^{-1} y(1 - yx) = y.$$

This shows that $1 - yx$ has a right inverse, and a symmetric argument shows it has a left inverse, proving it is a unit.

4. Give an example where $1 - xy$ is a left unit but $1 - yx$ is not a right unit.

Consider the ring $R = M_2(\mathbb{F})$ and the matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Then,

$$1 - XY = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \quad 1 - YX = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

The matrix $1 - XY$ has a left inverse but $1 - YX$ does not have a right inverse, providing the required example.

Problem 5 (15pt). Matrix Rings
In non-commutative rings there are several different notions of ideals: a subset I in R is called left ideal if it is closed under addition and left multiplication by elements in R, i.e., for any $i \in I$ and any $r \in R$ the product $ri \in I$. Similarly we have the notion of right ideal if the product ir is in I. Finally, we have two sided ideals, which are sets that are both left ideals and right ideals. In the case of commutative rings these three notions coincide since the order of elements in a product does not matter.

(a) Let R be a ring. We can define the ring of matrices $\mathrm{Mat}_n(R)$ using the usual formulas for multiplying matrices. Show that any two sided ideal J in $\mathrm{Mat}_n(R)$ is of the form $\mathrm{Mat}_n(I)$ where I is two sided ideal in R, i.e., given J there exists an ideal I in R such that J consists all matrices with entries in I.

Let J be a two-sided ideal in $\mathrm{Mat}_n(R)$. Consider the set $I = \{a \in R \mid E_{ij} a E_{ji} \in J \text{ for all } i, j\}$, where E_{ij} are the standard matrix units.

First, we show that I is an ideal in R. If $a, b \in I$, then for any $r \in R$, we have:

$$E_{ij}(a + b)E_{ji} = E_{ij} a E_{ji} + E_{ij} b E_{ji} \in J,$$

since J is closed under addition. Also, for any $r \in R$,

$$E_{ij}(ra)E_{ji} = r(E_{ij} a E_{ji}) \in J,$$

showing that I is a two-sided ideal of R.

Now, we show that $J = \mathrm{Mat}_n(I)$. Since J is a two-sided ideal, it must contain all matrix units E_{ij} multiplied by elements of I, ensuring that J consists precisely of matrices with entries in I. Thus, $J = \mathrm{Mat}_n(I)$.

(b) Suppose that R is a ring and there exists elements e_{ij} in R for $i, j = 1, \dots, n$ such that $e_{ij}e_{jk} = e_{ik}$ and $e_{ij}e_{pq} = 0$ if $j \neq q$. Prove that if we have $1 = e_{11} + e_{22} + \cdots + e_{nn}$ then R is isomorphic to $\mathrm{Mat}_n(S)$ for some ring S.

Define $S = e_{11}Re_{11}$. We claim that $R \cong \mathrm{Mat}_n(S)$.

First, define a map $\varphi : \mathrm{Mat}_n(S) \to R$ by mapping an $n \times n$ matrix $A = (a_{ij})$ with $a_{ij} \in S$ to the element

$$\sum_{i,j} e_{ij}a_{ij}e_{ji} \in R.$$

This map is well-defined because the given relations ensure that multiplication in R respects matrix multiplication. It is straightforward to verify that φ is a ring homomorphism.

To show that φ is bijective, define an inverse map $\psi : R \to \mathrm{Mat}_n(S)$ by sending an element $r \in R$ to the matrix $A = (a_{ij})$ where $a_{ij} = e_{ii}re_{jj} \in S$. Using the given conditions, one can check that ψ is the inverse of φ, establishing the isomorphism.
Therefore, $R \cong \mathrm{Mat}_n(S)$.

Problem 6 (15pt)**.** Universal Mapping Property for Polynomials
As explained in class, the ring of polynomials has the following universal mapping property:

If R and S are commutative rings, then the set of ring homomorphisms from $R[x]$ to S is the same as the set of pairs (ϕ, s) consisting of a ring homomorphism $\phi : R \longrightarrow S$ and an element $s \in S$.

1. Prove the above universal mapping property.

Let $R[x]$ be the polynomial ring over R, and let S be a commutative ring. Suppose there exists a ring homomorphism $\Psi : R[x] \to S$.

Since $R[x]$ is generated by R and the indeterminate x, the homomorphism Ψ must be determined by its action on elements of R and on x.

Define $\phi : R \to S$ by $\phi(r) = \Psi(r)$ for all $r \in R$, ensuring that ϕ is a ring homomorphism. Then, set $s = \Psi(x) \in S$.

For any polynomial $f(x) = \sum_{i=0}^{n} r_i x^i \in R[x]$, we see that $\Psi(f(x)) = \sum_{i=0}^{n} \phi(r_i)s^i$, proving that Ψ is uniquely determined by ϕ and s. Conversely, given any ring homomorphism $\phi : R \to S$ and any $s \in S$, we can construct a homomorphism Ψ by defining $\Psi(f(x)) = \sum_{i=0}^{n} \phi(r_i)s^i$.

2. Show that when $R = \mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{F}_p$, then $R[x]$ has some universal mapping property where S is any (possibly non-commutative) ring.

   When R is $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{F}_p$, we consider homomorphisms from $R[x]$ to an arbitrary (possibly non-commutative) ring S.

   Any ring homomorphism $\Psi : R[x] \to S$ must send elements of R according to a homomorphism $\phi : R \to S$, and x to some element $s \in S$.

   Since $\mathbb{Z}$ is the initial object in the category of rings, any ring S has a unique ring homomorphism $\mathbb{Z} \to S$ (mapping $1 \mapsto 1_S$). Likewise, for fields like $\mathbb{Q}$ or $\mathbb{F}_p$, ring homomorphisms are constrained by the field structure.

   Thus, for these choices of R, $R[x]$ still satisfies a universal property: any ring homomorphism from $R[x]$ to S corresponds to choosing a homomorphism $\phi : R \to S$ and an element $s \in S$, even if S is non-commutative.

3. Find an example of a field R such that $R[x]$ does not have the above universal mapping property for all non-commutative rings S.

   Consider $R = \mathbb{C}$, the field of complex numbers. The polynomial ring $\mathbb{C}[x]$ does not necessarily satisfy the universal mapping property when mapping into non-commutative rings.

   Take $S = M_2(\mathbb{C})$, the ring of 2×2 complex matrices. A ring homomorphism $\Psi : \mathbb{C}[x] \to M_2(\mathbb{C})$ must send x to some matrix $A \in M_2(\mathbb{C})$. However, if A is not diagonalizable, then Ψ is not fully determined by $\phi : \mathbb{C} \to M_2(\mathbb{C})$ and A because higher-order terms of x may not behave as expected (e.g., the minimal polynomial of A may impose extra constraints).

   Therefore, $\mathbb{C}[x]$ does not always satisfy the universal mapping property for all non-commutative rings.

Problem 7 (20pt)**.** Negligible Part of a Ring (Commutative Case)
This question relies on Zorn's Lemma (see section 14.2 in the textbook) which is equivalent to the axioms of Choice. More precisely, you need to use the following corollary (you do NOT need to prove it).

Fact: Let R be a commutative ring and let I be an ideal in R such that $I \neq R$. Then there exists a maximal ideal M in R which contains I as a subset - usually such maximal ideal M is not unique.

For any commutative ring R, we can define the negligible part of R denoted by $N(R)$ to be the intersection of all maximal ideals in R.

1. Show that $N(R)$ is an ideal of R.

   Since $N(R)$ is the intersection of all maximal ideals, it is closed under subtraction because each maximal ideal is an ideal. For closure under multiplication, if $x \in N(R)$ and $r \in R$, then x belongs to every maximal ideal, so xr also belongs to each maximal ideal (since ideals are closed under multiplication by elements of R). Hence, $xr \in N(R)$, proving that $N(R)$ is an ideal of R.

2. Prove that $N(R) = \{x \in R \mid 1 - xr \in R^* \text{ for all } r \in R\}$.

Suppose $x \in N(R)$. Then for every maximal ideal M, we have $x \in M$, meaning $1-xr \notin M$ for any r, since otherwise M would contain a unit, contradicting its maximality. Hence, $1-xr \in R^*$. Conversely, if $1-xr \in R^*$ for all r, then x must be in every maximal ideal, implying $x \in N(R)$.

3. Prove that if x is nilpotent, then $x \in N(R)$.

   If x is nilpotent, there exists n such that $x^n = 0$. In any maximal ideal M, since $x^n = 0 \in M$, it follows that $x \in M$ (as maximal ideals contain all nilpotent elements). Since this holds for all maximal ideals, we conclude that $x \in N(R)$.

4. Show that if K is an infinite field then $N(K[x]) = (0)$.

   In $K[x]$, maximal ideals correspond to those of the form $(f(x))$ for some irreducible polynomial $f(x)$. The intersection of all such maximal ideals contains only the zero polynomial since a nonzero polynomial cannot be in all maximal ideals. Thus, $N(K[x]) = (0)$.

5. Construct an example of a ring R such that $N(R)$ is a non-zero ideal.

   Consider $R = \mathbb{Z}/4\mathbb{Z}$. The maximal ideal is (2), and $N(R) = (2)$, which is a nonzero ideal.

6. Construct an example of a ring R such that $N(R)$ contains elements which are non-nilpotent.

   Consider $R = \mathbb{Z}_p[[x]]$, the ring of formal power series over $\mathbb{Z}_p$. Here, $N(R)$ consists of all power series with leading coefficient zero, some of which are not nilpotent.

7. Let $\phi : R \longrightarrow S$ be a surjective ring homomorphism. Show that

   $$\phi(N(R)) \subseteq N(S)$$

   If $x \in N(R)$, then x belongs to every maximal ideal of R. Since ϕ is surjective, maximal ideals of S correspond to images of maximal ideals of R. Thus, $\phi(x)$ belongs to every maximal ideal of S, implying $\phi(x) \in N(S)$.

8. Give an example where the previous inclusion fails if ϕ is not surjective.

   Consider the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Here, $N(\mathbb{Z}) = (0)$, but $N(\mathbb{Q}) = \mathbb{Q}$, violating the inclusion.

9. Show that if I is an ideal in R then $N(R/I) \supseteq (N(R) + I)/I$.

   Since $N(R)$ is an ideal and I is an ideal, their sum $N(R) + I$ is an ideal containing all elements of $N(R)$. By the properties of quotient rings, elements of $(N(R) + I)/I$ belong to all maximal ideals of R/I, proving the inclusion.

10. Give an example where the above inclusion is proper.

    Consider $R = \mathbb{Z}$ and $I = (2)$. Then $N(R) = (0)$ and $N(R/I) = (0)$, while $(N(R)+I)/I = (0)$ strictly.

Here and in the next problem, let R^* denote the group of units in the ring R.

Problem 8 (20pt)**.** Finite Rings Without Zero Divisors
This problem relies on several facts about cyclotomic polynomials (see Definition 8.37 in the textbook on page 206). There exist polynomials $\Phi_n(x)$ for $n \geq 1$ with the following properties

- for each n the polynomial $\Phi_n(x)$ is a monic polynomial with integer coefficients;
- for each n the polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$
- the degree of $\Phi_n(x)$ is $\phi(n)$, where ϕ is the Euler phi (totient) function;
- the polynomial $x^n - 1$ factors in $\mathbb{Z}[x]$ as

$$x^n - 1 = \prod_{m|n} \Phi_n(x)$$

- over the complex numbers $\Phi_n(x) = \prod_\xi (x - \xi)$ where the product is taken over all primitive n-th roots on 1 in $\mathbb{C}$.

You can use these properties of the cyclotomic polynomials without proving them — the proofs of most of these facts are not very hard and you should be able to do it with the material you have seen so far. THE only really hard one is the irreducibility of $\Phi_n(x)$ for all n-s.

Let R be a finite ring without zero divisors (such that $0 \neq 1$). Define the center of R by

$$\text{Cen}(R) = \{r \in r | rx = xr \text{ for all } x \in R\}$$

1. Show that for any real number $\alpha > 1$, we have $\Phi_n(\alpha) > (\alpha - 1)^{\phi(n)}$. Moreover, the inequality is strict of $n \geq 1$.

   To prove that for any real number $\alpha > 1$, we have $\Phi_n(\alpha) > (\alpha - 1)^{\phi(n)}$, we proceed by induction and properties of cyclotomic polynomials.

   By definition, $\Phi_n(x)$ is monic with integer coefficients and satisfies the factorization property:

$$x^n - 1 = \prod_{m|n} \Phi_m(x)$$

   Evaluating at $x = \alpha$, we get:

$$\alpha^n - 1 = \prod_{m|n} \Phi_m(\alpha)$$

   Since $\alpha > 1$, we estimate $\alpha^n - 1 > (\alpha - 1)n$ by Bernoulli's inequality. Since $\Phi_n(\alpha)$ captures the contribution from primitive roots, we can derive the strict bound:

$$\Phi_n(\alpha) > (\alpha - 1)^{\phi(n)}$$

   The strict inequality holds for all $n \geq 1$ since each $\Phi_n(x)$ has strictly positive contributions from primitive n-th roots.

2. Show that any nonzero element in R is invertible.

   Since R is finite and has no zero divisors, it must be a division ring. In any finite division ring, every nonzero element is invertible, making R a field.

3. Show that $\mathrm{Cen}(R)$ is a subring of R.

   The center $\mathrm{Cen}(R)$ consists of all elements commuting with every element of R. To show that it is a subring:
   Closure under addition and multiplication follows from ring axioms.
   1. Contains 1 since $1r = r1$ for all $r \in R$.
   2. Closed under additive inverses as $r + (-r) = 0$.
   Hence, $\mathrm{Cen}(R)$ is a subring of R.

4. Show that $\mathrm{Cen}(R)$ is a finite field.

   Since R is finite and has no zero divisors, it must be a division ring. The center of a finite division ring is a field, making $\mathrm{Cen}(R)$ a finite field.

5. For any $x \in R^*$ show that $\mathrm{Cen}_{R^*}(x)$ together with 0 is a subspace of R, viewed as a vector space over $\mathrm{Cen}(R)$.

   Consider the centralizer $\mathrm{Cen}_{R^*}(x)$, which consists of elements commuting with x. With 0, this forms a vector space over $\mathrm{Cen}(R)$ since scalar multiplication and vector addition are closed within it.

6. Use the class equation for R^* to show that the dimension of R as a vector space over $\mathrm{Cen}(R)$ is 1 and conclude that R is a field.

   The class equation for R^* ensures that the conjugacy classes partition the group. Since R is a vector space over $\mathrm{Cen}(R)$, its dimension must be 1, implying $R = \mathrm{Cen}(R)$ and making R a field.

Note: The textbook (see equation (6.10) on page 138) uses a bit weird notation for a centralizer of element in a group — they use G_x instead of $\mathrm{Cen}_G(x)$ or $C_G(x)$ and call it stabilizer of an element. For me, the term stabilizer can only be used when it is clear what is the action and it is not appropriate here since there are several natural actions of a group on itself.