2023 Fall Honors Algebra Exercise 3 (due on October 26)

For submission of your homework, please finish the 25 True/False problems, and choose 10 questions from the standard ones and 5 questions from the more difficult ones. Mark the question numbers clearly.

[A] = Artin, [DF] = Dummit and Foote, [DN] = Ding and Nie (Chinese), [H] = Hungerford.

All rings contain 1 and $1 \neq 0$ in these rings. Moreover, homomorphisms always take 1 to 1.

3.1. **True/False questions.** (Only write T or F when submitting the solutions.) The letter p always refers to a prime number, and n a positive integer.

(1) If G is an abelian group of order n, the for any divisor d of n, G contains a subgroup of order d.

(2) The commutator subgroup of a simple group G must be G itself. (careful)

(3) Let G be a group acting on a set X. If $g_1, g_2 \in G$ and $x \in X$, then $g_1 \cdot x = g_2 \cdot x$ implies $g_1 = g_2$.

(4) Let G be a p-group acting on a finite set X. Then the number of fixed points of the action is congruent modulo p to $\#X$.

(5) Let p be a prime number and $\alpha \in \mathbb{N}$. Then every group of order $2p^\alpha$ is solvable.

(6) All Sylow p-subgroups of a group G are isomorphic.

(7) If H is a subgroup of G, then $N_G(H)$ is a normal subgroup of G.

(8) A semi-direct product of two finite abelian groups is solvable.

(9) If a finite group G has order p^n, then its solvable length $\leq n$.

(10) A finite nilpotent group is the direct product of its Sylow subgroups (of different primes)

(11) Let G be a group of order p^n. Then for each $i = 1, \dots, n-1$, subgroups of G of order p^i are conjugate of each other.

(12) A p-group G of order p^n contains a subgroup of order of p^i for every $i = 0, \dots, n$.

(13) Every group of order 42 has a normal subgroup of order 7.

(14) Every group of prime-power order is solvable.

(15) If G/H is abelian, then the commutator subgroup G' of G contains H.

(16) Let R be a commutative ring and $R' \subseteq R$ is a subring. Then R/R' admits a natural ring structure.

(17) Let R be a commutative ring and let I and J be ideals. Then IJ is the ideal consisting of elements of the form ab with $a \in I$ and $b \in J$.

(18) Let R be a (not necessarily commutative) ring, evaluating polynomials at $x = a \in R$ defines a homomorphism $R[x] \to R$, $f(x) \mapsto f(a)$.

(19) A zero-divisor in a commutative ring with unity may have a multiplicative inverse.

(20) The Hamilton quaternion $\mathbb{H}$ has only two ideals: 0 and $\mathbb{H}$.

For (21)–(25) below, let $\varphi : R \to R'$ be a surjective homomorphism of commutative rings.

(21) if $a \in R$ is a zero-divisor, then $\varphi(a) \in R'$ is a zero-divisor;

(22) if R is an integral domain, then $\varphi(R) = R'$ is an integral domain;

(23) if R' is an integral domain, then R is an integral domain;

(24) if $u \in R$ is a unit, then $\varphi(u)$ is a unit in R';

(25) if $\varphi(u) \in R'$ is a unit, then u is a unit in R.

3.2. **Warm-up questions.** (Do not submit solutions to these questions)

Problem 3.2.1. [DF, page 136, problems 1 and 2]

(1) Prove that if P is a Sylow p-subgroup of G and H is a subgroup of G containing P then P is a Sylow p-subgroup of H. Give an example to show that, in general, a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G.

(2) Prove that if H is a subgroup of G and Q a Sylow p-subgroup of H, then gQg^{-1} is a Sylow p-subgroup of gHg^{-1} for all $g \in G$.

Problem 3.2.2. Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of S_4.

Problem 3.2.3. [DF, page 147, problem 18]

Prove that if $\#G = 200$ then G is not simple.

Problem 3.2.4. Compute the lower and upper series for D_8.

Problem 3.2.5. Let N be a normal subgroup of G. Suppose that both N and G/N are solvable. Then G is solvable.

Problem 3.2.6. Let $\varphi : G \to H$ be a surjective homomorphism. Show that the image of a Sylow p-subgroup is a Sylow p-subgroup.

Problem 3.2.7. Explicitly write down all one-dimensional representations of the dihedral group D_{2n}. (The answer depends on the parity of n.)

Problem 3.2.8.

(1) Let R be a commutative ring with 1, if $a^2 = a$ is an idempotent element, then aR and $(1-a)R$ both naturally have ring structure (what are the "1"s?) Moreover, we have
$$R \cong aR \times (1-a)R.$$

(2) A ring R is a *Boolean ring* if $a^2 = a$ for all $a \in R$, so that every element is *idempotent*. Show that every Boolean ring is commutative.

Problem 3.2.9. Let R be a commutative ring and $n \in \mathbb{N}$. Show that the following two rings are isomorphic.
$$\mathrm{Mat}_n(R[x]) \cong \big(\mathrm{Mat}_n(R)\big)[x]$$
(Think: what exactly do we need to prove?)

Problem 3.2.10. [DF, page 231, problem 7]

The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$. Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

Problem 3.2.11. [DF, page 256, problem 6]

Prove that R is a division ring if and only if its only left ideals are (0) and R. (The analogous result holds when "left" is replaced by "right.")

3.3. **Standard questions.** (Choose 10 problems to submit)

Problem 3.3.1. [DF, page 147, problem 23]
Prove that if $\#G = 462$ then G is not simple.

Problem 3.3.2. Prove that every group of order $5 \cdot 7 \cdot 47$ is abelian and cyclic.

Problem 3.3.3. A group of order 72 is not a simple group.

Problem 3.3.4. [DF, page 147, problem 33]
Let $P \in \mathrm{Syl}_p(G)$ and assume $N \trianglelefteq G$. Prove that $P \cap N$ is a Sylow p-subgroup of N. Deduce that PN/N is a Sylow p-subgroup of G/N.

Problem 3.3.5. [DF, page 147, problem 28]
Let G be a group of order 1575. Prove that if a Sylow 3-subgroup of G is normal then a Sylow 5-subgroup and a Sylow 7-subgroup are normal. In this situation prove that G is abelian.

Problem 3.3.6. [DF, page 147, problem 16]
Let $\#G = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

Problem 3.3.7. [DF, page 147, problem 35]
Let $P \in \mathrm{Syl}_p(G)$ and let $H \leq G$. Prove that $gPg^{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$. Give an explicit example showing that $hPh^{-1} \cap H$ is not necessarily a Sylow p-subgroup of H for any $h \in H$ (in particular, we cannot always take $g = 1$ in the first part of this problem, but we can when H was normal in G).

Problem 3.3.8. Let S_{p^2} be the permutation group of p^2 elements. Show that the Sylow p-subgroup of S_{p^2} is isomorphic to a semi-direct product $(\mathbf{Z}_p)^p \rtimes_\varphi \mathbf{Z}_p$. Specify the homomorphism $\varphi : \mathbf{Z}_p \to \mathrm{Aut}((\mathbf{Z}_p)^p)$ that defines this semi-direct product. (In fact, this is a *wreath product* $\mathbf{Z}_p \wr \mathbf{Z}_p$.)

Problem 3.3.9. [A, page 230, §2, problem 12]
Prove or disprove: A nonabelian simple group cannot operate nontrivially on a set containing fewer than five elements.

Problem 3.3.10. Suppose that p is the smallest prime integer which divides $\#G$. Prove that a subgroup H of index p is normal.

Problem 3.3.11. [A, page 231, §3, problem 10]
Let B be the subgroup of $G = \mathrm{GL}_n(\mathbb{C})$ of upper triangular matrices, and let $U \subset B$ be the set of upper triangular matrices with diagonal entries 1. Prove that $B = N_G(U)$ and $B = N_G(B)$.

Problem 3.3.12. [DF, page 198, problem 12]
Compute the upper and lower central series of A_4.

Problem 3.3.13. [DF, page 198, problem 9]
Prove that a finite group G is nilpotent if and only if whenever $a, b \in G$ with $\gcd(|a|, |b|) = 1$ then $ab = ba$.

Problem 3.3.14. [DF, page 188, Theorem 1(3)]
Let P be a group of order p^a and H a normal subgroup of P of order p^b. Then for every $c \in \{0, \ldots, b\}$, H contains a subgroup of order p^c that is *normal in G*.

Problem 3.3.15. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the power set of X). Define addition and multiplication on $\mathcal{P}(X)$ by

$$A + B = (A \backslash B) \cup (B \backslash A) \quad \text{and} \quad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

(1) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as rings of sets).
(2) Prove that this ring is commutative, has an identity and is a Boolean ring. (See Problem 3.2.8 for the definition of Boolean rings.)

(Hint: of course, one may really use subsets as elements of $\mathcal{P}(X)$, but the proof might look nasty. Maybe think about the indicator function of the subsets.)

Problem 3.3.16. [DF, page 267, problem 1]

Let R be a ring with identity $1 \neq 0$. 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.

Problem 3.3.17. (1) Show that the units in the product of commutative rings is the product of sets of units, i.e. for two commutative unital rings R_1 and R_2, we have $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$. Show that this is also a group isomorphism.

(2) From this deduce that, if $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of a positive integer, we have

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

(3) Show that for each odd prime p_i, the group of units $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ is a cyclic group of order $p_i^{\alpha_i - 1}(p_i - 1)$. (Optional)

Problem 3.3.18. In a ring R, write $Z(R)$ for its center, namely $Z(R) = \{r \in R \,|\, ar = ra \text{ for any } a \in R\}$.

(1) What is the center of $\mathrm{Mat}_{n\times n}(\mathbb{C})$?
(2) If A and B are rings. Show that $Z(A \times B) = Z(A) \times Z(B)$.
(3) Let $n_1, \ldots, n_r$ be positive integers. What is the center of the ring

$$\prod_{i=1}^{r} \mathrm{Mat}_{n_i}(\mathbb{C}).$$

Problem 3.3.19. Show that, in an commutative ring R, for two ideals $I, J \subseteq R$, we have

$$IJ \subseteq I \cap J.$$

Give an example of an integral domain R, and two ideals I, and J such that the inclusion is strict.

3.4. **More difficult questions.** (Choose 5 questions to submit.) Some of the proof has reference; it is okay to read the proof there and reproduce it on your homework.

Problem 3.4.1. Let p be a prime and let $\mathbb{F}_p$ denote the field of p elements.

(1) Find the order of $\mathrm{GL}_n(\mathbb{F}_p)$.
(2) Give a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.
(3) How many Sylow p-subgroups does $\mathrm{GL}_n(\mathbb{F}_p)$ have? (Compute explicitly.)
(4) Verify that the number of Sylow p-subgroups satisfies the Sylow's third theorem.

Problem 3.4.2. [DF, page 148, problem 44]
Let p be the smallest prime dividing the order of a finite group G. If $P \in \mathrm{Syl}_p(G)$ and P is cyclic, prove that $N_G(P) = C_G(P)$.

Problem 3.4.3 (Yau contest 2015)**.** Let p and q be two distinct prime numbers. Let G be a non-abelian finite group satisfying the following conditions:

(a) all nontrivial elements have order either p or q;
(b) The q-Sylow subgroup H_q is normal and is a nontrivial abelian group.

Show in steps the following statement:

> The group G is of the form $\mathbf{Z}_p \ltimes (\mathbf{Z}_q)^n$, where the action of $1 \in \mathbf{Z}_p$ on $\mathbf{Z}_q^n \simeq \mathbb{F}_q^n$ is given by a matrix $M(1) \in \mathrm{GL}_n(\mathbb{F}_q)$. each of whose eigenvalue is a primitive p-th root of unity.

(1) Let H_p denote a p-Sylow subgroup of G. Show that its inclusion into G induces an isomorphism $H_p \cong G/H_q$, and that $G \simeq H_p \ltimes H_q$.
(2) Let $M : H_p \to \mathrm{Aut}(H_q) \simeq \mathrm{GL}_n(\mathbb{F}_q)$ be the homomorphism induced from the conjugations. Show that for each $1 \neq a \in H_p$, $M(a)$ is semisimple and each of whose eigenvalue is a primitive p-th root of unity. In particular M is injective.
(3) Show that if two nontrivial elements $a, b \in H_p$ commute with each other, then $a = b^n$ for some $n \in \mathbb{N}$, and that $H_p \simeq \mathbf{Z}_p$.
(4) Complete the solution of the problem.

Problem 3.4.4. [Alibaba contest, 2020]
Find all finite groups G satisfying the following conditions:

- the order of G is the product of distinct primes, i.e. $\#G = p_1 \cdots p_m$ for some distinct primes $p_1, \dots, p_m$; and
- all non-trivial elements of G have prime order, that is, the order of every element belongs to $\{1, p_1, \dots, p_m\}$.

(Note: The answer depends on m; for example, when $m = 2$, there are many such G; you need to classify them.) (I don't particular enjoy this problem because I don't feel it contain more information than a tricky problem.)

Problem 3.4.5. [DF, page 198, problem 8]
Prove that if p is a prime and P is a non-abelian group of order p^3, then $|Z(P)| = p$ and $P/Z(P) \cong \mathbf{Z}_p \times \mathbf{Z}_p$.

Problem 3.4.6. Recall that the commutator subgroup $[G, G]$ of a group G is *generated* by the commutators $a^{-1}b^{-1}ab$ for $a, b \in G$. It is not true in general that every element in $[G, G]$ is of the form of a commutator. Here is one example from MathOverflow (question number 7811, due to Derek Holt).

Let p be a prime number and $n \in \mathbb{N}$. Consider a group G generated by elements a_i ($1 \leq i \leq n$), such that

- $a_i^p = 1$ for every i,
- for $1 \leq i < j \leq n$, the commutator $b_{ij} = a_i^{-1}a_j^{-1}a_ia_j$ is central in G, and satisfies $b_{ij}^p = 1$.

Prove the following statements:

(1) The commutator subgroup $[G, G]$ has order $p^{n(n-1)/2}$ and is generated by b_{ij}.
(2) On the other hand, show that elements of the form $[x, y]$ with $x, y \in G$ can have at most p^{2n} elements.
(3) Deduce from this that for any fixed $k > 0$, by choosing n sufficiently large, we can find G such that not all elements of $[G, G]$ are products of at most k commutators.

Problem 3.4.7. [DN, page 79–80]

A different proof of First Sylow Theorem following the book by Shisun Ding and Lingzhao Nie. (In fact, we prove a seemingly stronger statement.) Let G be a finite group or order $n = p^r \cdot m$ with p a prime number, $r, m \in \mathbb{N}$ such that $p \nmid m$. Let $k \leq r$ be an integer, then G contains a subgroup of order p^k. (When $k = r$, we recover First Sylow Theorem.)

First prove an elementary lemma. When $n = p^r \cdot m$ with $p^r || \, n$,

$$p^{r-k} || \binom{n}{p^k}.$$

Next, consider the set A of subsets of G or cardinality p^k. Then G acts on A by left translation:

$$g \cdot \{x_1, \ldots, x_{p^k}\} = \{gx_1, \ldots, gx_{p^k}\}.$$

Show that there is an orbit whose cardinality is not divisible by p^{r-k+1}.

From this, deduce that the stabilizer group of one element in this orbit is a subgroup of order p^k.

Remark: It is hard to compare this proof with the proof given in class. We shall see shortly that by studying subgroups of p-groups, every p-group is solvable, and thus contains a subgroup of every smaller p-power order. So the statement in Dummit–Foote is essentially not weaker than Ding–Nie's statement. Personally, I feel Dummit–Foote's argument is slightly more natural than Ding–Nie's(?)

Problem 3.4.8. [A, page 232, §5, problem 3]

Let G be a group of order 30.

(1) Prove that either the Sylow 5-subgroup K or the Sylow 3-subgroup H is normal.
(2) Prove that HK is a cyclic subgroup of G.
(3) Classify groups of order 30.

Problem 3.4.9. A different proof of simplicity of A_n. See for example [DN, page 66, Theorem 9]

Step 1: Prove that A_n is generated by 3-cycles. (check directly that the product of any two transpositions can be rewritten as a product of 3-cycles.)

Step 2: Show that it is enough to show that every nontrivial normal subgroup H of A_n contains one 3-cycles.

Step 3: Discuss fixed points of elements in H. Take an element τ with most fixed points and show that τ has exactly $n - 3$ fixed points, and thus a 3-cycle.

Problem 3.4.10. Let F be a field consider the group $B_n(F)$ of upper-triangular invertible matrices, and its subgroup of strict upper-triangular matrices

$$U_n(F) = \left\{ \begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 1 & a_{23} & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \;\middle|\; a_{ij} \in F \right\}$$

(1) Compute the upper and lower central series of $B_n(F)$ and $U_n(F)$.
(2) Compute the derived series of $B_n(F)$.

Optional: From these computation, we see that $B_n(F)$ is a solvable group whereas $U_n(F)$ is a nilpotent group. In fact, for $U_n(F)$, we may replace the field F by $\mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$. In this case, can you make explicit why $U_n(\mathbb{Z}/m\mathbb{Z})$ is the product of its Sylow subgroups?

Problem 3.4.11. (from a discussion with Junyi Xie)

Let p be a prime number. Consider the following subset of polynomials

$$S = \left\{ \sum_{n \geq 0} a_n x^{p^n} \;\middle|\; a_n \in \mathbb{F}_p \right\}.$$

Show that S is closed under composition $f \circ g(x)$.

Prove that S together with the natural addition and composition (not the multiplication) is a ring, and isomorphic to the polynomial ring $\mathbb{F}_p[x]$.

(Can you construct a natural map from $\mathbb{F}_p[x] \to S$ that is easy to describe and involves the Frobenius map? Here Frobenius map is $f(x) \mapsto f(x)^p$; but when we are in a ring where $p = 0$, raising to pth power preserves addition and multiplication.)

Problem 3.4.12. [DN, page 129, problem 1]

Let R be a ring with $1 \neq 0$. For two elements $a, b \in R$, if $1 - ab$ is a unit, then $1 - ba$ is a unit.

(I have a nice explanation of the proof, but I don't want to ruin it; so I leave the hint to the end of the file. It's up to you whether to use it.)

Problem 3.4.13. Let $A, B \in \mathbb{Q}^\times$ be rational numbers. Consider the quaternion ring

$$D_{A,B,\mathbb{R}} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

in which the multiplication satisfies relations: $\mathbf{i}^2 = A$, $\mathbf{j}^2 = B$, and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$.

(1) Represent $\mathbf{jk}$, $\mathbf{ik}$, $\mathbf{k}^2$ in terms of elements in $D_{A,B,\mathbb{R}}$.
(2) When $A, B > 0$, show that $D_{A,B,\mathbb{R}}$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{R})$, given by

$$\mathbf{i} \leftrightarrow \begin{pmatrix} \sqrt{A} & 0 \\ 0 & -\sqrt{A} \end{pmatrix}, \quad \mathbf{j} \leftrightarrow \begin{pmatrix} 0 & B \\ 1 & 0 \end{pmatrix}.$$

(3) Show that $D_{A,B,\mathbb{R}}$ is isomorphic to $\mathbb{H}$ if and only if $A, B < 0$, and is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ if at least one of A and B is positive.
(4) Why is $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ not isomorphic to $\mathbb{H}$?

Problem 3.4.14. Let $A, B \in \mathbb{Q}^\times$ be rational numbers. Consider the quaternion ring

$$D_{A,B,\mathbb{Q}} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Q}\}$$

in which the multiplication satisfies relations: $\mathbf{i}^2 = A$, $\mathbf{j}^2 = B$, and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$.

(1) Show that if either A or B is a square in $\mathbb{Q}$, then $D_{A,B,\mathbb{Q}}$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{Q})$.
(2) Prove that $D_{A,B,\mathbb{Q}}$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{Q})$ if and only if $x^2 = Ay^2 + Bz^2$ has a nonzero (meaning not all zero) solution in $\mathbb{Q}$.

Problem 3.4.15. [Alibaba 2021]

Let p be a prime number and let $\mathbb{F}_p$ be the finite field with p elements. Consider an automorphism τ of the polynomial ring $\mathbb{F}_p[x]$ given by

$$\tau(f)(x) = f(x+1).$$

Let R denote the subring of $\mathbb{F}_p[x]$ consisting of those polynomials f with $\tau(f) = f$. Find a polynomial $g \in \mathbb{F}_p[x]$ such that $\mathbb{F}_p[x]$ is a free module over R with basis $g, \tau(g), \dots, \tau^{p-1}(g)$ (in other words, every element of $\mathbb{F}_p[x]$ can be uniquely written as a "linear combination"

$$a_0 g + a_1 \tau(g) + \cdots + a_{p-1}\tau^{p-1}(g)$$

with $a_0, \dots, a_{p-1} \in R$.

<u>Hint for Problem 3.4.12</u>: Consider a Taylor expansion $(1-ab)^{-1} = 1 + ab + abab + \cdots$ and relate this to $(1-ba)^{-1}$. Then, you just have to make sense of what you have computed.