This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 1

Solve and submit your solutions of the following problems. Note that the last problem is worth the same as the previous 5! Also note that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, September 19, 2025 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Determine which of the following operations are associative:

1. On $\mathbb{Z}$, $a * b := a - b$.
2. On $\mathbb{R}$, $a * b := a + b + ab$.
3. On $\mathbb{Q}$, $a * b := (a + b)/5$.
4. On $\mathbb{Z} \times \mathbb{Z}$, $(a, b) * (c, d) := (ad + bc, bd)$.
5. On $\mathbb{Q} \setminus \{0\}$, $a * b := a/b$.

Q2 (10 points)

Let $S := [0, 1)$ and on it define

$$a * b := \begin{cases} a + b & \text{if } a + b < 1 \\ a + b - 1 & \text{otherwise.} \end{cases}$$

Show that with this operation S is an Abelian (commutative) group.

Q3 (10 points)

Let $\sigma = [13, 2, 15, 14, 10, 6, 12, 3, 4, 1, 7, 9, 5, 11, 8]$ and $\tau = [14, 9, 10, 2, 12, 6, 5, 11, 15, 3, 8, 7, 4, 1, 13]$ be permutations in S_{15}. The cycle decomposition of σ is $(1, 13, 5, 10)(3, 15, 8)(4, 14, 11, 7, 12, 9)$. Find the cycle decompositions of τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

Q4 (10 points)

Let $\mathbb{Q}[\sqrt{2}]$ denote the set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

1. Show that $\mathbb{Q}[\sqrt{2}]$ is a group under addition.
2. Show that $\mathbb{Q}[\sqrt{2}] \setminus \{0\}$ is a group under multiplication.

Q5 (10 points)

Let G and H be group, and let $G \times H$ be taken with the operation $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$.

1. Show that $G \times H$ is a group. (It is called "the direct product of G and H").
2. If A and B are groups, show that $A \times B$ is Abelian if and only if both A and B are Abelian.
3. Prove that in $G \times H$, the elements $(g, 1)$ and $(1, h)$ commute.

Q6 (50 points)

Let $G = \langle g_1 = (1, 2, 3),\ g_2 = (2, 3, 4) \rangle \subset S_4$.

1. Use the NCGE algorithm discussed in class to write a "table of tricks" T for G.
2. Use T to determine $|G|$.
3. Use T to decide if $\sigma_1 = (12) \in G$.
4. Use T to decide if $\sigma_2 = (13)(24) \in G$.

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 2

Solve and submit your solutions of the following problems. Note that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Friday, September 26, 2025 11:59 pm (Eastern Daylight Time)

Late penalty
5% deducted per hour

Q1 (10 points)

1. Prove that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.
2. Let D_{2n} denote the group of symmetries of a regular n-gon, including rotations and reflections. Prove that the group D_{24} is not isomorphic to S_4.

Q2 (10 points)

Let G be a group. Prove that the map $\iota: G \to G$ defined by $\iota(g) = g^{-1}$ is always an anti-isomorphism, yet it is an isomorphism if and only if G is Abelian.

Q3 (10 points)

Describe in as simple terms as you can the automorphism group $\mathrm{Aut}((\mathbb{Q}, +))$.

Q4 (10 points)

If g is an element of a group G, the *order* $|g|$ of g is the least positive number n for which $g^n = 1$ (it may be ∞).

1. Prove that if x and y are conjugate, their orders are the same.
2. Prove that for any x and y, $|xy| = |yx|$.

Q5 (10 points)

Let G be a group. The *commutator* of two elements $a, b \in G$ is defined to be $[a, b] := aba^{-1}b^{-1}$. Let G' be the subgroup of G generated by all the commutators of pairs of elements of G. Show that G' is normal in G, that $A := G/G'$ is Abelian, and that any morphism from G into an Abelian group B factors through A.

$A = G/G'$ is often called "the Abelianization of G".

If you are not sure what "factors through" means, look it up.

Q6 (10 points)

Let G be a group. We've defined a map $C : G \to \mathrm{Aut}(G)$ by $C_h(g) := h^{-1}gh$. The image of this map, $\operatorname{im} C \subset \mathrm{Aut}(G)$, is called "the set of inner automorphisms of G".

Show that the set of inner automorphisms of a group G is a normal subgroup of the set $\mathrm{Aut}(G)$ of all automorphisms of G.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 3

Solve and submit your solutions of the following problems. Note that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, October 3, 2025 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (10 points)

1. A permutation $\sigma \in S_n$ has a cycle decomposition consisting of k cycles, of lengths $l_1, \dots, l_k$. What is the order of σ?
2. What is the smallest n for which S_n contains an element of order 18?
3. What is the maximal order of an element in S_{13}? In S_{26}?

Not for credit, and not so easy: If you're in the mood, figure out and plot the maximal order of an element in S_n as a function of n.

Q2 (10 points)

1. Let $\sigma, \tau \in S_n$ be permutations, and assume that σ has a cycle decomposition $\sigma = (a_{11}, a_{12}, \dots, a_{1l_1})(a_{21}, a_{22}, \dots, a_{2l_2}) \cdots (a_{k1}, a_{k2}, \dots, a_{kl_k})$. Prove that the cycle decomposition of $\sigma^\tau = \tau^{-1}\sigma\tau$ is $(\tau^{-1}a_{11}, \tau^{-1}a_{12}, \dots, \tau^{-1}a_{1l_1})(\tau^{-1}a_{21}, \tau^{-1}a_{22}, \dots, \tau^{-1}a_{2l_2}) \cdots (\tau^{-1}a_{k1}, \tau^{-1}a_{k2}, \dots, \tau^{-1}a_{kl_k})$.
2. Prove that two permutations σ_1 and σ_2 in S_n are conjugate iff the sequences of lengths of cycles in their cycle decompositions are the same (up to a permutation of these lengths).

Q3 (10 points)

1. Define a relation on permutations in S_n by $\sigma_1 \sim \sigma_2$ if σ_1 is a conjugate of σ_2. Show that $\sim$ is an equivalence relation.
2. We call the equivalence classes for the relation $\sim$ "the conjugacy classes of S_n". How many conjugacy classes are there in S_2? In S_3? In S_4? In S_5?

Q4 (10 points)

Let $\sigma \in G = S_{20}$ be a permutation whose cycle decomposition consists of one 5-cycle, two 3-cycles, and one 2-cycle. What is the order of the centralizer of σ, $C_G(\sigma) := \{\tau \in G : \sigma\tau = \tau\sigma\}$.

Q5 (10 points)

Let H be a subgroup of index 2 in a group G. Show that H is normal in G.

Hint. There's $G/H = \{gH : g \in G\}$, and there's $H\backslash G = \{Hg : g \in G\}$.

Q6 (10 points)

1. A group G is called *cyclic* if it is generated by a single element inside G. In other words, if there is a single element $a \in G$ whose set of powers, positive and negative, is G. Show that if G is cyclic then it is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}/n$ for some n
2. Show that if $G/Z(G)$ is cyclic then G is Abelian. (Recall that $Z(G)$ is the centre of G, the set of all elements in G that commute with all elements of G).

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 4

Solve and submit your solutions of the following problems. Note that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, October 10, 2025 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (10 points)

If $C \lhd A$ and $D \lhd B$, show that $(C \times D) \lhd (A \times B)$ and $(A/C) \times (B/D) \simeq (A \times B)/(C \times D)$.

Q2 (10 points)

If $A \lhd G$, $B \lhd G$, and $G = AB$, show that $G/(A \cap B) \simeq (G/A) \times (G/B)$.

Q3 (10 points)

Show that if A is Abelian and simple (though not necessarily finite), then $A \simeq \mathbb{Z}/p$ for some prime p.

Q4 (10 points)

A Group G is called "solvable" if there is a sequence of groups $G_0, G_1, \dots, G_n$ such that $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$ and such that G_i/G_{i+1} is Abelian for all $0 \leq i < n$.

1. Show that subgroups and quotient groups of solvable groups are solvable.
2. Show that if $N \triangleleft G$ and N and G/N are solvable, then so is G.

Q5 (10 points)

Show that if $n \geq 3$ then A_n contains a subgroup isomorphic to S_{n-2}.

Q6 (10 points)

1. Let G be a group such that there is an infinite chain of simple groups $G_1 \leq G_2 \leq G_3 \leq \cdots$ such that $G = \bigcup G_i$. Show that G is simple.
2. Let A_∞ be the set of bijections $\sigma : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ that are equal to the identity beyond some point and that are even up to that point. Namely, for each σ there is some n (which may depend on σ) such that if $k > n$ then $\sigma(k) = k$ and such that $\sigma|_{\underline{n}} \in A_n$, where A_n denotes the nth alternating group, a subgroup of S_n. Prove that A_∞ is an infinite simple group.

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 5

Solve and submit your solutions of the following problems. Note that the questions are not of equal values. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Saturday, October 18, 2025 11:59 pm (Eastern Daylight Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Recall that if $H < G$, the *index of H in G* is $(G : H) := |G/H|$.

Let G be a group and H_1 and H_2 be finite-index subgroups of G. Show that $H_1 \cap H_2$ is also of finite index in G and that $(G : H_1 \cap H_2) \leq (G : H_1)(G : H_2)$.

Hint. Might it be true that $g(H_1 \cap H_2) = (gH_1) \cap (gH_2)$? If so, so what?

Q2 (10 points)

Let G be a group and let H be a subgroup of finite index. Prove that there is a normal subgroup N of G, contained in H, so that $(G : N)$ is also finite. (Hint: Let $(G : H) = n$ and find a morphism $G \to S_n$ whose kernel is contained in H.)

Q3 (10 points)

If p is a prime, a p-group means "a group whose order is a power of p".

Let G be a finite group and p be a prime. Show that if H is a p-subgroup of G, then $(N_G(H) : H)$ is congruent to $(G : H)$ mod p. You may wish to study the action of H on G/H by multiplication on the left.

Q4 (15 points)

For each of the following G sets X, find all of the orbits $\mathcal{O}_i$, verify that $|X| = \sum_i |\mathcal{O}_i|$, and write each orbit $\mathcal{O}_i$ as a coset space G/H_i:

1. $G = S_3$, $X = \underline{3}^2$ with $\sigma((i,j)) = (\sigma i, \sigma j)$. (Recall that $\underline{3} = \{1,2,3\}$).
2. $G = S_3$, $X = \underline{3}^3$ with $\sigma((i,j,k)) = (\sigma i, \sigma j, \sigma k)$.
3. $G = S_n$, $X = 2^{\underline{n}} = \mathcal{P}(\underline{n})$, with the obvious action of permutations on subsets.

Q5 (15 points)

1. Let X be a transitive G-set, let $x, y \in X$ and let $g \in G$ and assume that $gx = y$. Prove that $\mathrm{Stab}_X(x) = \mathrm{Stab}_X(y)^g$.
2. Recall that a morphism $\phi : X \to Y$ between G-sets X and Y is a function $\phi : X \to Y$ that satisfies $g\phi(x) = \phi(gx)$ for every $g \in G$ and every $x \in X$. Let X and Y be two transitive G-sets, and let $x_0 \in X$ and $y_0 \in Y$. Show that the following two statements are equivalent:

- There is a morphism $\phi : X \to Y$ of G-sets that satisfies $\phi(x_0) = y_0$.
- $\mathrm{Stab}_X(x_0) < \mathrm{Stab}_Y(y_0)$.

3. For a G-set X, let $\mathrm{Aut}(X)$ denote the set of all invertible morphisms ϕ: $X \to X$. Let X be the transitive G-set G/H, for some $H < G$. Show that for every $x, y \in X$ there is a $\phi \in \mathrm{Aut}(X)$ such that $\phi(x) = y$ if and only if H is normal in G. In other words, the action of $\mathrm{Aut}(X)$ on X is transitive iff $H \lhd X$.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 6

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Friday, October 24, 2025 11:59 pm (Eastern Daylight Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Suppose $|G| = pq$ where p and q are prime, where $p < q$, and where p does not divide $q - 1$. Show that G is cyclic.

Q2 (10 points)

Suppose $|G| = 56$. Show that for some prime p dividing 56, G has a *normal* Sylow-p subgroup.

Hint. Otherwise there's not enough room for all the mess.

Q3 (10 points)

Prove if p is a prime and $p \mid |G|$, then G has an element of order p. (G may not be Abelian. In class we have proven the statement only for Abelian groups).

Q4 (10 points)

Find all the Sylow subgroups of S_3 and of $S_3 \times S_3$.

Q5 (10 points)

Find all the Sylow subgroups of S_4.

Q6 (10 points)

How many elements of order 7 are there in a simple group of order 168?

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 7

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, November 14, 2025 11:59 pm (Eastern Standard Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Let N and H be groups, and let $\phi : H \to \mathrm{Aut}(N)$ and $\psi \in \mathrm{Aut}(H)$ be given, and let $\phi' := \phi \circ \psi$. Show that $N \rtimes_{\phi'} H$ is isomorphic to $N \rtimes_{\phi} H$.

Note. "$\psi \in \mathrm{Aut}(H)$" is *correct*.

Q2 (10 points)

Let $N = \langle x \rangle / \langle x^7 \rangle$ and let $H = \langle y \rangle / \langle y^3 \rangle$, and let $\phi_1 : H \to \mathrm{Aut}(N)$ be given by $\phi_{1y}(x) = x^2$ and $\phi_2 : H \to \mathrm{Aut}(N)$ be given by $\phi_{2y}(x) = x^4$. Show that the groups $N \rtimes_{\phi_i} H$ for $i = 1, 2$ are isomorphic.

Q3 (10 points)

Let N, A, and B be groups, and let $H := A \times B$. Suppose $\psi : A \to \mathrm{Aut}(N)$ is given, and let $\phi := \psi \circ \pi_A$ where $\pi_A : A \times B \to A$ is the projection on the first factor. Show that $N \rtimes_\phi H$ is isomorphic to $(N \rtimes_\psi A) \times B$.

Note. An earlier version of this question had "$\psi : A \to \mathrm{Aut}(H)$". The correct version is as it is now, "$\psi : A \to \mathrm{Aut}(N)$".

Q4 (10 points)

Show that up to isomorphism and other then the direct product, there is only one group of the form $\mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 8

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Warning. It's a tough one! Give it the time that it deserves.

Due date
Friday, November 21, 2025 11:59 pm (Eastern Standard Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Suppose a group G is a product $A_1 \times \cdots \times A_m$, a group H is a product $B_1 \times \cdots \times B_n$, and a group K is a product $C_1 \times \cdots \times C_k$, with all the groups assumed to be Abelian.

1. Show that the set of homomorphisms $\Phi : G \to H$ can be put in a natural bijection with the set of $n \times m$ matrices (ϕ_{ij}), where ϕ_{ij} is a homomorphism $A_j \to B_i$. Let the matrix corresponding to Φ be denoted by M_Φ.
2. Suppose we also have a homomorphism $\Psi : H \to K$. Show that $M_{\Psi \circ \phi} = M_\Psi \cdot M_\Phi$, where the right hand side is a simple modification of the notion of matrix multiplication, which you have to make explicit.

Q2 (10 points)

Show that if r and r' are natural numbers and if A and A' are finite Abelian groups and $\Phi : \mathbb{Z}^r \times A \to \mathbb{Z}^{r'} \times A'$ is an isomorphism of groups, then $\phi_{11} : \mathbb{Z}^r \to \mathbb{Z}^{r'}$, in the sense of the previous question, is also an isomorphism.

Q3 (10 points)

Show that if the groups $\mathbb{Z}^r$ and $\mathbb{Z}^{r'}$ are isomorphic, then $r = r'$.

Q4 (10 points)

Show that if the groups $G = \prod_{i=1}^{m} \mathbb{Z} / p_i^{s_i} \mathbb{Z}$ and $H = \prod_{j=1}^{n} \mathbb{Z} / q_j^{t_j} \mathbb{Z}$ are isomorphic, where m, n, s_i, and t_j are natural numbers and where p_i and q_j are primes, then the sequences $((p_i, s_i))$ and $((q_j, t_j))$ are the same up to a permutation.

Hint. Pick another prime l and another natural number k, and compare the counts of elements of order l^k in G and in H.

Q5 (10 points)

Prove the uniqueness statement within the structure theorem of finite generated Abelian groups.

Q6 (14 points)

A tough bonus question.

1. (1 point) Show that if G is finitely generated, then so is its Abelianization A (see HW2 for "Abelianization").
2. (6 points) Let $F_2 = F(x, y)$ be the free group on two generators x and y, and let G be its subgroup consisting of the elements in which the total power of x is 0 (so $x^5 y^2 x^{-3} y^{-1} x^{-2}$ is in, but $x^5 y^2 x^{-3} y^{-1} x^{-1}$ is not). Show that G is generated by the (infinitely many) elements $\{y^{x^n} = x^{-n} y x^n : n \in \mathbb{Z}\}$.
3. (6 points) Show that the Abelianization of G is $\mathbb{Z}_{FS}^{\mathbb{Z}}$, where "FS" means "Finite Support".
4. (1 point) Deduce that there exists a finitely generated group that has a non-finitely generated subgroup.

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 9

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, November 28, 2025 11:59 pm (Eastern Standard Time)

Late penalty

5% deducted per hour

Q1 (10 points)

1. Prove that in any ring, $(-1)^2 = 1$.
2. Prove that even in a rng (a ring without a unit), for any a we have $(-a)^2 = a^2$.

(In this question, "prove" means "from the most basic axioms").

Q2 (10 points)

An "integral domain" is a commutative ring that has no zero divisors. Namely, a commutative ring in which $ab = 0$ implies that $a = 0$ or $b = 0$.

Prove that a finite integral domain is field.

Q3 (10 points)

A ring R is called *Boolean* if for every $a \in R$, we have that $a^2 = a$.

1. Prove that every Boolean ring is commutative.
2. Prove that if a Boolean ring is an integral domain, then it is isomorphic to $\mathbb{Z}/2$.

Q4 (10 points)

In a ring R, an element x is called "nilpotent" if for some positive n, $x^n = 0$. Let $\eta(R)$ be the set of all nilpotent elements of R.

1. Prove that if R is commutative then $\eta(R)$ is an ideal.
2. Find an example of a non-commutative ring R for which $\eta(R)$ is not an ideal.

Q5 (10 points)

Let A be a commutative ring. The constant term (the coefficient of x^0) of a polynomial $f \in A[x]$ is invertible in A and all its other coefficients are nilpotent. Show that f is invertible in $A[x]$.

Q6 (0 points)

No bonus question! I was going to ask: If J is a maximal ideal in ℓ^∞ containing the ideal $\{(a_i) : a_i \to 0\}$, prove that ℓ^∞/J is isomorphic to $\mathbb{R}$. But I couldn't find a simple enough proof, and so it's out.

Yet hey, during office hours today I learned a simple proof that $2 = 3$! This really does open up math to a whole world of new possibilities. Here's how it goes: Clearly, the group $2\mathbb{Z}$ is isomorphic to the group $3\mathbb{Z}$, as both of them are isomorphic to the group $\mathbb{Z}$. And so the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are isomorphic. As the former has 2 elements and the latter has 3 elements, it follows that $2 = 3$.

Is this truly a revolution in mathematics or am I making a silly mistake? Is there a moral to learn?

Ponder that, but no bonus is involved no matter what is your conclusion.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 10

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, January 16, 2026 11:59 pm (Eastern Standard Time)

Late penalty

5% deducted per hour

Q1 (10 points)

In class, your Prof. embarrassed himself by showing that he doesn't know long division. Help him out by proving the lemma below and explaining how it and induction imply that if f and g are polynomials in $F[x]$ (where F is a field) and $g \neq 0$ then there exist polynomials q and r such that $f = qg + r$ and $\deg(r) < \deg(g)$.

Lemma. If f and g are polynomials in $F[x]$ and $\deg(g) \leq \deg(f)$, then there exists some polynomial (in fact, monomial) h such that $\deg(f - hg) < \deg(f)$.

(Your Prof. then further embarrassed himself by showing that he can't do subtraction of two-digit numbers. That's beyond helping; don't bother trying).

Q2 (10 points)

A commutative domain R has the property that every $x \neq 0$ in it has a unique decomposition into a product of a unit and finitely many irreducible elements (up to a permutation and up to units). Show that in R every irreducible element is a prime and therefore R is a UFD.

Hint. If x is irreducible and it divides ab, then $zx = ab$, and a, b, and ab can be written as products of irreducibles in a unique way.

Q3 (10 points)

1. Show that the ideal $I = \langle 3,\, x^3 - x^2 + 2x - 1 \rangle$ inside the ring $\mathbb{Z}[x]$ is not principal.
2. Is $\mathbb{Z}[x]/I$ a domain?

Hint for 2. Show that $\mathbb{Z}[x]/I \cong (\mathbb{Z}/3)[x] \big/ \langle x^3 - x^2 + 2x - 1 \rangle$ and that $x^3 - x^2 + 2x - 1$ is prime in the UFD $(\mathbb{Z}/3)[x]$.

Q4 (10 points)

Prove that a ring R is a PID iff it is a UFD in which $\gcd(a, b) \in \langle a, b \rangle$ for every non-zero $a, b \in R$.

Hint. Fish an element with a minimal number of factors.

Q5 (10 points)

Show that the ring $R = \mathbb{Z}[i] = \{x + iy \colon x, y \in \mathbb{Z}\} \subset \mathbb{C}$ is Euclidean and hence a PID and a UFD. What are the units of that ring?

Hint for the first part. Let $a, b \in R$ and assume $b \neq 0$. You want to find a multiple of b that's near a, relative to a norm that you are yet to find. What does the set of all multiples of b by an integer looks like? By an imaginary integer? By an element of R?

Q6 (10 points)

In $\mathbb{Z}[i]$, find the greatest common divisor of 85 and $1 + 13i$, and express it as a linear combination of these two elements.

Q7 (10 points)

Explain why $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is not a UFD.

Q8 (0 points)

(Hard, for fun only) Show that the quotient ring $\mathbb{Q}[x, y]/\langle x^2 + y^2 - 1\rangle$ is not a UFD.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 11

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, January 23, 2026 11:59 pm (Eastern Standard Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Let q and p be primes in a PID R such that $p \nsim q$, let $\hat{p}$ denote the operation of "multiplication by p", acting on any R-module M, and let s and t be positive integers. On each of the R-modules R, $R/\langle q^t \rangle$, and $R/\langle p^t \rangle$, determine $\ker \hat{p}^s$ and $\operatorname{Im} \hat{p}^s$.

Q2 (15 points)

Definition. The "rank" of a module M over a commutative domain R is the maximal number of R-linearly-independent elements of M. (Linear dependence and independence is defined as in vector spaces).

Definition. An element m of a module M over a commutative domain R is called a "torsion element" if there is a non-zero $r \in R$ such that $rm = 0$. Let $\operatorname{Tor} M$ denote the set of all torsion elements of M. A module M is called a "torsion module" if $M = \operatorname{Tor} M$.

Let M be a module over a commutative domain R.

- Show that $\operatorname{Tor} M$ is always a submodule of M.
- Suppose that M has rank n and that $x_1, \dots x_n$ is a maximal set of linearly independent elements of M. Show that $\langle x_1, \dots x_n \rangle$ is isomorphic to R^n and that $M/\langle x_1, \dots x_n \rangle$ is a torsion module.
- Conversely show that if M contains a submodule N which is isomorphic to R^n for some n, and so that M/N is torsion, then the rank of M is n.

Q3 (10 points)

Show that the ideal $\langle 2, x \rangle$ in $R = \mathbb{Z}[x]$, regarded as a module over R, is finitely generated but cannot be written in the form $R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$.

Q4 (10 points)

Let M and N be modules over a ring R. In class we've defined their direct sum, $M \oplus N$. The purpose of this exercise to to give a "functional" definition of the direct sum, namely, a definition in terms of the properties that $M \oplus N$ ought to have, instead of the "constructive" definition that was given in class.

Definition An "abstract direct sum" of M and N is a triple $(S, \alpha : M \to S, \beta : N \to S)$ consisting of a module S and two morphisms α and β as indicated, such that whenever there is a triple $(P, a : M \to P, b : N \to P)$ there is a unique $\lambda : S \to P$ such that $a = \lambda \circ \alpha$ and $b = \lambda \circ \beta$.

- Prove that $M \oplus N$, along with the obvious inclusions $\alpha : M \to M \oplus N$ and $\beta : N \to M \oplus N$, is an abstract direct sum of M and N.
- Show that the abstract direct sum of M and N is unique. Namely, show that if $(S, \alpha : M \to S, \beta : N \to S)$ and $(S', \alpha' : M \to S', \beta' : N \to S')$ are both abstract direct sums of M and N, then S and S' are isomorphic.

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 12

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Friday, January 30, 2026 11:59 pm (Eastern Standard Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Find the tensor product of the $\mathbb{C}[t]$ modules $\mathbb{C}[t, t^{-1}]$ ("Laurent polynomials in t") and $\mathbb{C}$ (here t acts on $\mathbb{C}$ as 0).

Q2 (10 points)

Show that over any ring R, the tensor product of the R-module $R[x]$ with itself is the R-module $R[x, y]$.

Q3 (10 points)

Let V and W be finite dimensional vector spaces over a field F, and let $\mathrm{Hom}(V, W)$ denote the vector space of all linear transformations $V \to W$.

- Show that $\mathrm{Hom}(V, W)$ is isomorphic to $V^* \otimes W$ via a *natural* isomorphism. (The phrase *natural* has a formal definition within category theory, but stating it will take us too far away. So let's say that I just mean, "an isomorphism that does not depend on making any choices, such as a basis for V or for W).
- The assumptions in this question can be relaxed a bit, and one V and W can be allowed to be infinite dimensional. Which of them is it?

Q4 (10 points)

Let V be a finite dimensional vector space over a field F. There is an obvious bilinear map $e : V^* \times V \to F$, defined by $(\varphi, v) \mapsto \varphi(v)$. The functional definition of tensor products implies that there a unique linear map $t : V^* \otimes V \to F$ such that $t \circ \iota = e$, where ι is the standard map $V^* \times V \to V^* \otimes V$. In the light of the previous question, t can be interpreted as a linear map $t : \mathrm{Hom}(V, V) \to F$. Can you identify t as one of the well-known standard linear algebra operations? Which one? Why?

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 13

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Friday, February 13, 2026 11:59 pm (Eastern Standard Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Let M be a module over a PID R. Assume that M is isomorphic to $R^k \oplus R/\langle a_1\rangle \oplus R/\langle a_2\rangle \oplus \cdots \oplus R/\langle a_l\rangle$, with a_i non-zero non-units and with $a_1 \mid a_2 \mid \cdots \mid a_l$. Assume also that M is isomorphic to $R^m \oplus R/\langle b_1\rangle \oplus R/\langle b_2\rangle \oplus \cdots \oplus R/\langle b_n\rangle$, with b_i non-zero non-units and with $b_1 \mid b_2 \mid \cdots \mid b_l$. Prove that $k = m$, that $l = n$, and that $a_i \sim b_i$ for each i.

Q2 (10 points)

Let q and p be primes in a PID R such that $p \nsim q$, let $\hat{p}$ denote the operation of "multiplication by p", acting on any R-module M, and let s and t be positive integers.

1. For each of the R-modules R, $R/\langle q^t\rangle$, and $R/\langle p^t\rangle$, determine $\ker \hat{p}^s$ and $(R/\langle p\rangle) \otimes_R \ker \hat{p}^s$.

2. Explain why this approach for proving the uniqueness in the structure theorem for finitely generated modules fails.

Q3 (10 points)

Show that if R is a PID and S is a multiplicative subset of R then $S^{-1}R$ is also a PID.

Q4 (10 points)

Write $x^3 + x^2 + x + 1$ as a product of primes in the ring $(\mathbb{Z}/2)[x]$.

Q5 (10 points)

1. Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and assume that $a_n \neq 0$. Show that if $r/s \in \mathbb{Q}$ with r and s relatively prime satisfies $f(r/s) = 0$, then $r|a_0$ and $s|a_n$.
2. Formulate a version of this statement that is true over an arbitrary UFD R. No need to re-prove.

Q6 (0 points)

Just for fun (or maybe misery). Let x be some root of the equation

$$x^5 + (\sqrt[3]{2} - \sqrt{3})x^4 + \frac{1}{\sqrt{\sqrt{3} + \sqrt{5}}}x^3 - 1 = 0.$$

We know that x is algebraic over $\mathbb{Q}$. Find a polynomial f with rational coefficients whose roots include x. What is $\deg f$?

You will need to write some code to answer this question, or use some computer algebra system.

Why am I asking? This question demos that while the field $\mathbb{Q}$ of rational numbers is computer-practical, the field $\mathbb{A}$ of algebraic numbers is not. Short computations in $\mathbb{Q}$ have short answers. Short computations in $\mathbb{A}$ blow up exponentially.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 14

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date
Friday, February 27, 2026 11:59 pm (Eastern Standard Time)

Late penalty
5% deducted per hour

Q1 (10 points)

Suppose f and g are irreducible polynomials over a field F whose degrees are greater than 1 and are relatively prime. If a is a zero of f in some extension of F, show that g does not have a root in $F(a)$.

Q2 (10 points)

Find the degree and a basis for $\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)/\mathbb{Q}\left(\sqrt{15}\right)$ and for $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}\right)/\mathbb{Q}$.

Q3 (10 points)

Find an example of an extension E/F and elements $a, b \in E$ such that $F(a) \neq F(a,b) \neq F(b)$ and $[F(a,b) : F] < [F(a) : F][F(b) : F]$.

Q4 (10 points)

Find $\operatorname{minpoly}_{\mathbb{Q}}\left(\sqrt[3]{2} + \sqrt[3]{4}\right)$.

Q5 (10 points)

Let $a \in E/F$. Show that $[F(a) : F(a^3)] \leq 3$ and show by examples that $[F(a) : F(a^3)]$ can be 1, 2, or 3.

Q6 (10 points)

Suppose that $[E : \mathbb{Q}] = 2$. Show that there is an integer d such that $E \simeq \mathbb{Q}[\sqrt{d}]$ and d is not divisible by the square of any prime.

Q7 (0 points)

If you're in the mood, also solve the following questions, but do not submit your solutions. Note that some of these questions may be regarded as "warmups" for Q1-Q6:

1. Show that a field F is algebraically closed iff every irreducible polynomial in $F[x]$ is linear.
2. Let $E, m \in \mathbb{Q}$ with $m \neq 0$. Show that $\mathbb{Q}\left(\sqrt{E}\right) = \mathbb{Q}\left(\sqrt{m}\right)$ iff there is some $c \in \mathbb{Q}$ such that $E = mc^2$.
3. Suppose $[E : F]$ is prime. Show that for any $a \in E$, $F(a) = F$ or $F(a) = E$.
4. Let $a, b \in E/F$ and assume a and b are algebraic over F of degrees m and n respectively, where $\gcd(m,n) = 1$. Show that $[F(a,b) : F] = mn$.
5. Find $\operatorname{minpoly}_{\mathbb{Q}}\left(\sqrt{-3} + \sqrt{2}\right)$.
6. Let $0 \neq f \in F[x]$ and let $a \in E/F$. Show that if $f(a)$ is algebraic over F then so is a.
7. Show that $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[6]{2}\right)$.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 15

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, March 6, 2026 11:59 pm (Eastern Standard Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Let F be a field and let $f \in F[x]$ be a polynomial of degree 2 or 3. Show that f is irreducible iff it has no roots in F.

Q2 (10 points)

Show that the polynomial $x^2 - 2$ is irreducible in $\mathbb{F}_3[x]$. Use that to give a complete descrption of a field E that has 9 elements. Namely, for some basis $B = \{u_1, u_2\}$ of $E/\mathbb{F}_3$, compute all the products $u_i u_j$ as linear combinations of elements of B. Likewise, compute the inverses of all the non-zero linear combinations of elements of B.

Q3 (10 points)

Let G be a finite Abelian group with the property that $\forall k \, |\{g \in G : g^k = e\}| \leq k$.

1. Show that if $G \simeq \prod \mathbb{Z}/p_i^{s_i}$, then the primes p_i are distinct.
2. Show that G is cyclic.
3. Show that the multiplicative group of a finite field is always cyclic. You may wish to consider the roots of the polynomials $x^k - 1$.

Q4 (10 points)

1. Let R be a UFD and let $p \in R$ be a prime. Let $f \in R[x]$ and let $\bar{f}$ be the image of f in $(R/\langle p \rangle)[x]$. Assume that $\deg \bar{f} = \deg f$ and that $\bar{f}$ is irreducible in $(R/\langle p \rangle)[x]$. Show that f is irreducible in $Q[x]$, where Q is the field of fractions of R.
2. Use $p = 5$ to show that $21x^3 - 3x^2 + 2x + 8$ is irreducible in $\mathbb{Q}[x]$.
3. Yet note that the same polynomial is not irreducible mod 2.

Q5 (10 points)

1. Show that a polynomial $f(x)$ is irreducible if and only if the polynomial $f(x+1)$ is irreducible.
2. For a prime p, show that the pth cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 16

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, March 20, 2026 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (20 points)

1. By elementary means, prove that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$
2. Show that $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$ is a splitting extension of degree 4.
3. Identify $G = \mathrm{Gal}\big(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}\big)$.
4. Draw the lattice of subfields of $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ and the corresponding lattice of subgroups of its Galois group G.

Q2 (30 points)

Let $\omega := \exp(2\pi i/7)$ be a 7th root of 1.

1. Possibly using Q5 of HW15, show that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$.
2. Show that $\mathbb{Q}(\omega)/\mathbb{Q}$ is a splitting extension.
3. Using the automorphism ϕ of $\mathbb{Q}(\omega)/\mathbb{Q}$ defined by extending $\omega \mapsto \omega^3$, show that $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is isomorphic to the cyclic group of order 6, C_6.

4. Draw the lattice of subgroups of the Galois group G.
5. Draw the corresponding lattice of subfields of $\mathbb{Q}(\omega)$.
6. I believe that $\alpha := \omega + \omega^6$ and $\beta := \omega + \omega^2 + \omega^4$ are primitive elements of the two interesting subfields of $\mathbb{Q}(\omega)$. Prove me right!
7. How did I come up with α and β?

Q3 (20 points)

Let $E := \mathbb{Q}(x^4 + 1)$.

1. Identify $G = \mathrm{Gal}(E/\mathbb{Q})$.
2. Find all the subfields of E.
3. Find the automorphisms of E whose fixed fields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(i)$.
4. Is there an automorphism of E whose fixed field is $\mathbb{Q}$?

Q4 (10 points)

Let E/F be a finite extension of a field F whose characteristic is 0 (not necessarily a splitting extension!). Show that there are only finitely many fields in between F and E.

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 17

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

Due date

Friday, March 27, 2026 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Let $f \in \mathbb{Q}[x]$ be cubic. If $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ is cyclic of order 3, show that all the roots of f are real.

Q2 (10 points)

Give an example of fields $\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset F_3$ (with all the inclusions strict) such that $[F_3 : F_0] = 8$ and such that if $i < j$ then F_j/F_i is splitting, with one exception, that F_2/F_0 is not splitting.

Q3 (10 points)

Determine $\mathrm{Gal}\big(\mathbb{Q}(x^4 - 14x^2 + 9)\big/\mathbb{Q}\big)$.

Q4 (15 points)

Let p be a prime. Prove that $\mathrm{Gal}\big(\mathbb{Q}(x^p - 2)\big/\mathbb{Q}\big)$ is isomorphic to the group of matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$ and $a \neq 0$.

Q5 (15 points)

Let E/F be a splitting extension with $\mathrm{char}(F) = 0$, let $a \in E$, let $G := \mathrm{Gal}(E/F)$, and let $H := \mathrm{Gal}(E/F(a))$. Show that $\prod_{\beta \in G/H}(x - \beta(a))$ is the minimal polynomial of a over F. (First make sure that "$\beta(a)$" makes sense for $\beta \in G/H$, noting that G/H may not even be a group).

Q6 (20 points)

Let E/F be a splitting extension with $\mathrm{char}(F) = 0$ and let $G := \mathrm{Gal}(E/F)$. Define the "norm function" $N : E \to E$ by $N(a) := \prod_{\sigma \in G} \sigma(a)$ and the "trace function" $T : E \to E$ by $T(a) := \sum_{\sigma \in G} \sigma(a)$.

1. Prove that for any $a \in E$, $N(a) \in F$ and $T(a) \in F$, so really, $N, T : E \to F$.
2. Prove that N is multiplicative, $N(ab) = N(a)N(b)$ and T is additive, $T(a + b) = T(a) + T(b)$.
3. What are N and T if E/F is $\mathbb{C}/\mathbb{R}$?
4. If $E = F(\sqrt{D})$ is a degree 2 extension, show that $N(a + b\sqrt{D}) = a^2 - Db^2$ and $T(a + b\sqrt{D}) = 2a$.
5. If $m(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0 \in F[x]$ is the minimal polynomial of $a \in E$ over F and $n := [E : F]$, show that $N(a) = (-1)^n c_0^{n/d}$ and $T(a) = -\frac{n}{d}c_{d-1}$.

Ready to submit?

- Please ensure all pages are in order and rotated correctly before you submit
- You will not be able to resubmit your work after the due date has passed.

Please wait...

This is a preview of what students will see when they are submitting the assignment. Interactive features are disabled.

Homework Assignment 18

Solve and submit your solutions of the following problems. Note also that the late policy is very strict - you will lose 5% for each hour that you are late. In other words, please submit on time!

That's our last assignment! Hurray!

Due date

Friday, April 3, 2026 11:59 pm (Eastern Daylight Time)

Late penalty

5% deducted per hour

Q1 (10 points)

Show that using a ruler and a compass alone, you cannot construct a regular heptagon (7-gon) and a regular nonagon (9-gon).

Q2 (10 points)

A angle trisector (angtri) is a device that given two lines a and b that meet at a point P, allows one to draw a further line c, such that the angle between a and c is one-third the angle between a and b (see notes below). Show that using only a ruler, a compass, and an angtri, one cannot construct a regular hendecagon (11-gon).

Note 1. We don't care that there are two angles between a and b, an acute one and an obtuse one. If you can trisect one you can easily trisect the other.

Note 2. One can make a mechanical angtri rather easily, though of course, using more than a ruler and a compass. In the old times people used to wear mechanical watches. If you brute-force move the minutes hand of a mechanical watch, the hours hand will move 12 times slower. Multiply by 4 and you've made a mechanical angtri.

Q3 (10 points)

1. Show that if a 19° angle is given, you can cut it into 19 equal parts using only a ruler and a compass.
2. Now do the same so elegantly that it will make you smile.
3. Yet show that, unfortunately, a 19° angle cannot be constructed with a ruler and a compass.

Q4 (10 points)

Working over $\mathbb{Q}$, in class we saw that $\mathrm{Gal}(f = 3x^5 - 15x + 5) \simeq S_5$. Find another polynomial with the same property. Multiplying f by a unit is cheap, so please avoid that. Also avoid $f \mapsto f(ax+b)$, $f \mapsto x^5 f(1/x)$, and combinations of all of these operations.

Ready to submit?

→ Please ensure all pages are in order and rotated correctly before you submit

→ You will not be able to resubmit your work after the due date has passed.

Please wait...