

Archive for
MATH 523, Algebra 1, Fall 2025

Bilkent University, Laurence Barker, 27 January 2025.

Source file: arch523fall25.tex

page 2: Course specification.

page 4: Homeworks with solutions.

page 10: Midterm

page 11: Solutions to Midterm.

page 12: Group theory reprise.

page 13: Solutions to group theory reprise.

page 14: Final.

page 15: Solutions to Final.

Course specification

MATH 523, *Algebra 1*, Fall 2025

Laurence Barker, Bilkent University. Version: 22 December 2025.

Instructor: Laurence Barker, Office SA 129, barker at fen dot bilkent dot edu dot tr.

Course Texts: Required:

- David S. Dummit, Richard M. Foote, “Abstract Algebra”, 3rd edition, (Wiley, New York, 2004). PDF internet downloads available.

Recommended:

- Joseph Rotman, “Galois Theory”, 2nd edition (Springer, New York, 1998).
- I. Martin Isaacs, “Algebra, a Graduate Course”, (Brooks/Cole, Pacific Grove, 1993).

See also supplementary material on my homepage

<http://www.fen.bilkent.edu.tr/~barker/fenis2.html>

and on Moodle.

Classes: Mondays 15:30 - 17:20, Thursdays 10:30 - 11:20, room SA-Z03.

Office Hours: For now, Thursday 11:30 - 12:20, in my office, room SA-129. The time might change later.

Weekly Syllabus

The format below is, *Week number; Monday date; Topics and Dummit–Foote section numbers.*

1: 15 Sept. Groups reviewed, Lagrange’s Theorem, Orbit-Stabilizer Equation, 3.2, 4.1.

2: 22 Sept. Groups reviewed, Sylow’s Theorem, simplicity of A_n , 4.5, 4.6.

3: 29 Sept. Euclidian domains, principal ideal domains, 8.1, 8.2.

4: 6 Oct. Unique factorization domains, 8.3.

5: 13 Oct. Polynomial rings over UFDs, 9.1 - 9.5.

6: 20 Oct. Field extensions, ruler-and-compass constructions, 13.3.

7: 27 Oct. *No class on Monday.* Splitting fields, 13.4.

8: 3 Nov. Separable extensions, cyclotomic extensions, 13.5, 13.6.

9: 10 Nov. Galois extensions. 14.1.

10: 17 Nov. The Fundamental Theorem of Galois Theory, 14.2.

11: 24 Nov. Composite extensions, the Primitive Element Theorem, 14.4.

12: 1 Dec. The Galois group of a cyclotomic extension, 14.5.

13: 8 Dec. Calculating Galois groups, 14.6.

14: 15 Dec. Group theory review.

15: 22 Dec. *No class on Thursday.* Galois theory review.

Assessment:

A minimum of 75% attendance is required.

- Homeworks: 15%.
- Midterm, closed book face-to-face: 40%.
- Final, closed book face-to-face: 45%.

Midterm schedule: Monday, 24 November, 15:30 - 17:30, classroom hours, those 2 lecture hours to be made up from spare hours. Location to be arranged.

Final schedule: Monday, 29 December, 14:00 - 16:30, room SBZ 04.

Midterm Retake: Friday, 2 January, 14:00 - 16:00, room SA Z02.

The Midterm Retake, group theory reprise, is for students who obtained less than 50% in the Midterm. The maximum recorded revised Midterm mark is 50%.

FZ criteria: Dreadful midterm and homework performance.

Speaking: All speaking in class must address everyone in the room.

Class Announcements: All students, including any absentees from a class, will be deemed responsible for awareness of class announcements.

Homework and Some Solutions

MATH 523, *Algebra 1*, Fall 2025, Laurence Barker

version: 22 December 2025

Homework 1: *due Monday 13 October at or before start of lecture.*

Some exercises from Dummit–Foote, not marked:

- Section 4.5, questions 32, 33, 34, 35 on page 147.
- Section 4.6, questions 1, 2, 3 on page 151.

Solutions to the following questions are to be handed in by **Thursday, 9th October**.

I intend to choose three of them and to mark only those three.

Exercise 1.1: Recall, from lectures, that a permutation group is a pair of sets (H, S) equipped with a binary operation $H \times S \rightarrow S$ satisfying certain axioms. Recall that, for a group G , a G -set is a set T equipped with a binary operation $G \times T \rightarrow T$ satisfying certain axioms.

- (a) Show that, given such (H, S) , then H acquires a group structure and S becomes an H -set.
- (b) Explain why not every G -set arises as a permutation group.

Exercise 1.2: Let Ω be a set of operators. State versions of the second and third isomorphism theorems for Ω -groups.

Exercise 1.3: Let G be any group and let $I, J \leq G$. Show that there exists an isomorphism of G -sets $G/I \cong G/J$ if and only if I and J are G -conjugate.

Exercise 1.4: Using the simplicity of the alternating group A_5 , give an inductive proof of the simplicity of A_n for all $n \geq 5$. (Such a proof can be found in Section 4.6 of the main textbook.)

Exercise 1.5: Find all the subgroups of D_8 , the dihedral group with order 8. (Anecdotally, in a Qualifying Exam, at a university far far away, a candidate was able to show that a certain Galois extension had Galois group D_8 . But the candidate was unable to then apply the Fundamental Theorem of Galois Theory because he or she was unable to classify the subgroups of D_8 .)

Exercise 1.6: Consider the symmetric group S_4 with degree 4.

- (a) Find all the subgroups of S_4 up to conjugacy. (Hint: Make use of Sylow’s theorem. If S_4 seems too big, warm up with some smaller groups, say, S_3 and A_4 .)
- (b) Which of those subgroups act transitively on the natural S_4 -set $\{1, 2, 3, 4\}$? (This question amounts to a classification of the different kinds of irreducible quartic equation over $\mathbb{Q}$.)

Exercise 1.7: Find, up to isomorphism, all the groups with order 15 and all the groups with order 21.

Exercise 1.8: Classify, up to isomorphism, the groups G such that the automorphism group $\text{Aut}(G)$ is trivial. (Hint: You might find it helpful to make use of an equivalent of the Axiom of Choice.)

Homework 2: due Thursday, 13 November, at or before start of lecture.

Exercise 2.1: Very generally $\text{rank}(G)$, the **rank** of any group G , can be defined as the minimum cardinality of a generating set for G . Let p be a prime and P a finite p -group. Recall, the rank $r = \text{rank}(P)$ is the dimension of the $\mathbb{F}_p$ -vector space $P/\Phi(P)$, where $\Phi(P)$ denotes the Frattini subgroup. Fixing r and letting P run over all the finite p -groups with rank r , what is the minimum possible number of cyclic subgroups of P ?

Exercise 2.2: Consider the ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$.

(1) Show that $\mathbb{Z}[i]$ is a Euclidian domain with norm $N(a + ib) = a^2 + b^2$.

(2) Explain why $\mathbb{Z}[i]$ is a unique factorization domain.

(3) Classify the prime ideals of $\mathbb{Z}[i]$.

Note: Details of this can be found everywhere, including the notes, also the Wikipedia article on *Gaussian integers*. But it is anyway instructive to work through the material.

Exercise 2.3: Let $f(X) = X^4 + 3X^2 + 3X + 9$ as a polynomial over $\mathbb{Z}$ and over $\mathbb{Q}$.

(a) Show that $f(X)$ has no rational roots.

(b) Factorize the image of $f(X)$ in $\mathbb{F}_2[X]$.

(c) Using parts (a) and (b), show that $f(X)$ is irreducible over $\mathbb{Q}[X]$.

Exercise 2.4: Over the field $\mathbb{F}_3$ with order 3, completely factorize $X^8 - 1$. Hence find all the irreducible monic polynomials with degree 2 in $\mathbb{F}_3[X]$.

Exercise 2.5★: For rings R and S , the setwise direct product $R \times S$ can be viewed as a ring in an evident way. Often, this ring is denoted by $R \oplus S$. Describe two different ways in which the ring $R \times S = R \oplus S$ can be regarded as a universal. Hint: You may need to think carefully about the appropriate way to define the notion of a ring homomorphism. (Warning, this is a tricky question that would not be suitable for a written exam. It is intended to stimulate thought.)

Solutions 2:

Solution 2.1: We shall show that the minimum number of cyclic subgroups of P is the number

$$m_r = 1 + \frac{p^r - 1}{p - 1} = 2 + \sum_{s=1}^{r-1} p^s.$$

First suppose P is elementary abelian. Then, aside from the trivial subgroup of P , every cyclic subgroup of P is of order p and has $p - 1$ generators. On the other hand, every non-identity element of P generates a cyclic subgroup with order p . Since $|P| = p^r$, the number of cyclic subgroups with order p is $(p^r - 1)/(p - 1)$. Therefore, in this case, the number of cyclic subgroups of P is exactly m_r .

Now suppose that P is not elementary abelian. For each cyclic subgroup C of $P/\Phi(P)$, we choose a generator $x\Phi(P)$ and let $C' = \langle x \rangle$, which is a cyclic subgroup of P . The function $C \mapsto C'$ is injective. So P has at least m_r cyclic subgroups. The proof is now complete.

Incidentally, if $\Phi(P) \neq 1$, then $\Phi(P)$ has at least 2 cyclic subgroups. So the minimum m_r is attained only when P is elementary abelian.

Comment: When P is elementary abelian, we can regard P as an r -dimensional vector space over the field $\mathbb{F}_p$. Then the cyclic subgroups of P are precisely the subspaces with dimension 0 or 1. But this conversion to a problem in linear algebra really just amounts to a change of terminology.

Solution 2.2: Part (1). Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Write $\alpha/\beta = u + iv$ with $u, v \in \mathbb{Q}$. Let U and V be integers such that $|u - U| \leq 1/2 \geq |v - V|$. We have

$$\alpha = (U + iV)\beta + X + iY$$

for some $X, Y \in \mathbb{Z}$. Then

$$X + iY = ((u - U) + i(v - V))\beta.$$

So $N(X + iY) = ((u - U)^2 + (v - V)^2)N(\beta) \leq N(\beta)/2 < N(\beta)$.

Part (2). Every Euclidian domain is a unique factorization domain.

Part (3). We shall show that the prime ideals of $\mathbb{Z}[i]$ are as follows:

- The principal ideals (p) where p is a prime congruent to 3 modulo 4.
- The prime ideals having the form $(a + ib)$ where a and b are integers such that $a^2 + b^2 = p$ and either $p = 2$ or else p is a prime congruent to 1 modulo 4. For each p , there are exactly 2 such ideals, namely $a + ib$ and $a - ib$.

For each rational prime p , we must examine the prime factorization of p in $\mathbb{Z}[i]$. Note that $N(p) = p^2$. For any $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$. The units in $\mathbb{Z}[i]$ are the elements ± 1 and $\pm i$. These are precisely the elements of $\mathbb{Z}[i]$ that have norm 1. Putting all those observations together, we deduce that either p is prime in $\mathbb{Z}[i]$ or else $p = st$ where s and t are primes in $\mathbb{Z}[i]$ with $N(s) = N(t) = p$.

Any sum of two squares is congruent to 0 or 1 or 2 modulo 4. Therefore, if $p \equiv 3$ modulo 4, then p is prime in $\mathbb{Z}[i]$. We have $2 = (1 + i)(1 - i)$ and $N(1 + i) = N(1 - i) = 2$. In view of our classification of the units of $\mathbb{Z}[i]$, the primes $1 + i$ and $1 - i$ are non-associate. So $(1 + i)$ and $(1 - i)$ are distinct prime ideals dividing (2) .

Now suppose $p \equiv 1$ modulo 4. Since $\mathbb{Z}/p$ is a field, the unit group $(\mathbb{Z}/p)^\times$ is cyclic. Since $|(\mathbb{Z}/p)^\times| = p - 1$, which is divisible by 4, there exists an integer $1 < x < p$ such that $x^2 \equiv -1$

modulo p . The integer $x^2 + 1 = (x + i)(x - i)$ is divisible by p . If p divides $x + i$, say $x + i = p(a + ib)$, then p divides x , which is impossible. So p does not divide $x + i$ and, similarly, p does not divide $x - i$. Therefore, p is not prime, in other words, $p = st$ as above. Writing $s = a + ib$, then $a^2 + b^2 = N(s) = p$. Hence $p = (a + ib)(a - ib)$ as a product of primes.

The argument is now complete. Note that, in the process, we have recovered Fermat's Two Squares Theorem, which asserts that a rational prime p is a sum of two squares if and only if p is congruent to 1 or 2 modulo 4.

Solution 2.3: Part (a). Since none of the integers $\pm 1, \pm 3, \pm 9$ is a root for $f(X)$, the rational root test implies that $f(X)$ has no rational roots.

Part (b). The image of $f(X)$ factorizes as a product of irreducibles

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

Note that $X^3 + X^2 + 1$ does not have root 0 or 1 and must therefore be irreducible.

Part (c). For a contradiction, suppose $f(X)$ is not irreducible over $\mathbb{Q}[X]$. By Gauss' Lemma, $f(X)$ is not irreducible over $\mathbb{Z}[X]$. By part (a), $f(X) = g(X)h(X)$ as a product of 2 irreducible polynomials over $\mathbb{Z}$ with degree 2. Since $\mathbb{F}_2(X)$ is a unique factorization domain, the image of $g(X)$ or $h(X)$ in $\mathbb{F}_2(X)$ must divide $X^3 + X^2 + 1$. That contradicts part (b).

Solution 2.4: Over $\mathbb{F}_3$, we have $X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$. So

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + X - 1)(X^2 - X - 1)$$

which is easily seen to be a product of irreducibles. Every irreducible monic polynomial of degree 2 over $\mathbb{F}_3$ has splitting field $\mathbb{F}_9$. But every nonzero element of $\mathbb{F}_9$ is a root of $X^8 - 1$. So the irreducible monic polynomials of degree 2 over $\mathbb{F}_3$ are precisely the irreducible factors of $X^8 - 1$ with degree 2, and those polynomials are $X^2 + 1$ and $X^2 + X - 1$ and $X^2 - X - 1$.

Solution 2.5: This question is a rather whimsical one.

One way of realizing $R \times S \cong R \oplus S$ as a universal is to see it as a product. The canonical span $R \leftarrow R \times S \rightarrow S$ is a universal for spans $R \leftarrow U \rightarrow S$ in the sense that there is always a unique map $U \rightarrow R \times S$ that commutes with the legs.

In the category of rings, the coproduct is the free product, not the direct product. However, allowing ring maps that do not preserve unity elements, then there is a canonical cospan $R \rightarrow R \times S \leftarrow S$. This is a universal for those cospans $R \rightarrow V \leftarrow S$ such that the images of R and S in V commute and intersect trivially. Indeed, for such cospans, there is always a unique map $R \times S \rightarrow V$ that commutes with the legs.

Homework 3: *To be placed in my mailbox by Thursday, 25 December, 09:00.*

Exercise 3.1: Let G and H be groups and let $\theta : G \rightarrow \text{Aut}(H)$ be a group homomorphism. We define the **semidirect product** of G over H with respect to θ , written as $G \ltimes_{\theta} H$ or just $G \ltimes H$, to be $G \times H$ as a set, with operation given by

$$(g', h')(g, h) = (g'g, \theta(g^{-1})(h')h) .$$

Here, $\theta(g^{-1})(h')$ denotes the image of h' under the automorphism $\theta(g^{-1})$ of H . Confirm that this is a group operation.

Exercise 3.2: Prove the following theorem. It is called the **semidirect product recognition theorem**. Given subgroups $G, H \leq F$ such that $G \cap H = 1$ and $H \trianglelefteq F$, then GH is a subgroup of F and $GH = G \ltimes H$ with G acting on H by conjugation.

Exercise 3.3: Let p be a prime.

(a) Show that, up to isomorphism, there exists a unique nonabelian semidirect product having the form $C_p \ltimes C_{p^2}$.

(b) Find the number of conjugacy classes of $C_p \ltimes C_{p^2}$.

Exercise 3.4: We consider only spans of sets. Recall that, given sets A and B , a **span** $A \leftarrow B$ is a diagram having the form

$$A \xleftarrow{e_1} E \xrightarrow{e_2} B$$

where E is a set called the **apex**, also e_1 and e_2 are functions called the **legs**. We understand two spans $A \leftarrow B$ to be the same provided there is a bijection between the apexes that commutes with the legs. Recall, composition of spans is by a pullback construction. By direct use of explicit construction of pullbacks for sets, without appealing to any abstract theory about pullbacks, prove that composition of spans is associative.

Solutions 3:

Solution 3.1: Sketch. By direct calculation, it is straightforward to check associativity and inversion.

Solution 3.2: Since $H \trianglelefteq F$, we have $GH \leq F$. Given $g_1, g_2 \in G$ and $h_1, h_2 \in H$ such that $g_1 h_1 = g_2 h_2$, then $g_2^{-1} g_1 = h_2 h_1^{-1} \in G \cap H = \{1\}$, hence $g_1 = g_2$ and $h_1 = h_2$. So there exists a bijection $GH \leftrightarrow G \times H$ given by $gh \leftrightarrow (g, h)$. We have

$$g_1 h_1 g_2 h_2 = g_1 g_2 g_2^{-1} h_1 g_2 h_2 \leftrightarrow (g_1 g_2, g_2^{-1} h_2 g_2 h_1) .$$

Therefore, $GH \cong G \ltimes H$.

Solution 3.3: Part (a). There is an isomorphism $(\mathbb{Z}/p^2)^\times \cong \text{Aut}(C_{p^2}) \cong$ given by $r \leftrightarrow \alpha_r$ where $\alpha_r(x) = x^r$ for $x \in C_{p^2}$. We have $|(\mathbb{Z}/p^2)^\times| = \phi(p^2) = p(p-1)$. So the unique Sylow p -subgroup of $\text{Aut}(C_{p^2})$ is cyclic with order p . The required conclusion now follows.

Part (b). The number of conjugacy classes is $p^2 + p - 1$. We shall show that, in fact, this conclusion holds for any non-abelian group G with order p^3 . We have $|Z(G)| = p$. For any $x \in G - Z(G)$, the conjugacy class $[x]$ has size $|[x]| \geq p$. But $C_G(x) \leq \langle Z(G), x \rangle$, hence $|C_G(x)| \geq p^2$. By the orbit-stabilizer equation, those two inequalities are equalities. So all the conjugacy classes contained in $G - Z(G)$ have size p . The number of such conjugacy classes is $|G - Z(G)|/p = p^2 - 1$. Of course, the number of singleton conjugacy classes is p .

Solution 3.4: We write the specified span as a triple (e_1, E, e_2) . We use a similar notation for cospans. Let A, B, C, D be sets. Let

$$e = (e_1, E, e_2) : A \leftarrow B, \quad f = (f_1, F, e_2) : B \leftarrow C, \quad g = (g_1, G, g_2) : C \leftarrow D$$

be spans. To form the composite ef , we form the pullback span (h_1, H, h_2) of the cospan (e_2, B, f_1) . As an explicit construction, we can put

$$H = \{(x, y) \in E \times F : e_2(x) = f_1(y)\},$$

taking h_1 and h_2 to be the restrictions of the projections from $E \times F$. Then $ef = (e_1 h_1, H, f_2 h_2)$. To form $(ef)g$, we pullback H and G to form a subset $J \subseteq E \times F \times G$. We have $(ef)g = (\ell_1, J, \ell_2)$ where $\ell_1(x, y, z) = e_1(x)$ and $\ell_2(x, y, z) = g_2(z)$ for $(x, y, z) \in J$. The construction of $e(fg)$ is similar, involving a pullback i of (f_2, C, g_1) . We have

$$\begin{aligned} J &= \{(w, z) \in H \times G : f_2 h_2(w) = g_1(z)\} \\ &= \{(x, y, z) \in E \times F \times G : e_2(x) = f_1(y), f_2(y) = g_1(z)\}. \end{aligned}$$

In view of the symmetry, $(ef)g = e(fg)$.



Midterm

24 November 2025, LJB

1: (15 marks.) Let G be a finite group with generators a and b such that $a^5 = b^4 = 1$ and $bab^{-1} = a^2$. Find a set of representatives g of the conjugacy classes of G and, for each representative g , evaluate the size $|C_G(g)|$ of the centralizer $C_G(g)$ and the size $|[g]_G|$ of the conjugacy class $[g]_G$. Present your results in clear tabular form, say, with g in the first column, $|C_G(g)|$ in the second column, $|[g]_G|$ in the third column. (Marks will be lost if the results are scattered across a tract of discussion.)

2: (25 marks.) For the symmetric group S_6 find:

(a) The number of Sylow 5-subgroups.

(b) The number of Sylow 3-subgroups.

(c) The number of Sylow 2-subgroups.

3: (25 marks.) Let G be a finite group, let p be the smallest prime divisor of $|G|$ and let $H < G$ such that $|G|/|H| = p$. Show that $H \triangleleft G$. (Hint: consider a group homomorphism $G \rightarrow \text{Sym}(L)$, where L is the set of left cosets of H in G .)

4: (10 marks.) Let n be any positive integer. Show that there exists a field K such that $[K : \mathbb{Q}] = n$. (Give enough detail to make it clear why $\mathbb{Q}$ cannot be replaced by an arbitrary field.)

5: (25 marks.) Show that $\mathbb{Z}[\sqrt{3}]$ is a Euclidian domain. (Hint: consider the function $a + b\sqrt{3} \mapsto |a^2 - 3b^2|$.)

Solutions to Midterm

1: We have $a^{-1}ba = ab$. That, and similar equalities, shows that the conjugacy classes are $[1] = \{1\}$ and $[a] = A - \{1\}$ and $[b^j] = Ab^j$ for $j \in \{1, 2, 3\}$. We have $C_G(a) = \langle a \rangle$ and $C_G(b^j) = \langle b \rangle$. The data in the presented table is now clear.

$[g]$	$ C_G(g) $	$ [g] $
$[1]$	1	1
$[a]$	5	4
$[b]$	4	5
$[b^2]$	4	5
$[b^3]$	4	5

2: For $p \in \{2, 3, 5\}$, let n_p denote the number of Sylow p -subgroups of S_6 . Let Ω denote the natural permutation set for S_6 .

Part (a). The Sylow 5-subgroups are isomorphic to C_5 . To choose a 5-cycle g in S_6 , there are 6 choices for the unique element of Ω fixed by g , then $4!$ choices for the action of g on the other elements of Ω . In each Sylow 5-subgroup, the number of 5-cycles is 4. Therefore, $n_5 = 4!6/4 = 36$.

Part (b). The Sylow 3-subgroups of S_6 are $C_3 \times C_3$, acting on Ω with 2 orbits with size 3. Each 3-cycle belongs to a unique Sylow 3-subgroup. In each Sylow 3-subgroup, the number of 3-cycles is 4. The number of 3-cycles in S_6 is $6 \cdot 5 \cdot 4 / 3 = 120$. Therefore, $n_3 = 120 / 4 = 30$.

Part (c). The Sylow 2-subgroups of S_6 have the form $D_8 \times C_2$, where $D_8 \times 1$ acts on an orbit with size 4 while $1 \times C_2$ acts on an orbit with size 2. There are $6 \cdot 5 / 2 = 15$ choices for the subgroup $1 \times C_2$. That choice having been fixed, then the number of choices for the D_8 subgroup is equal to the number of Sylow 2-subgroups of S_4 , which is 3. Therefore, $n_2 = 15 \cdot 3 = 45$.

3: Let $\theta : G \rightarrow \text{Sym}(L)$ such that $\theta(g)(xH) = gxH$ for $g, x \in G$. Let $K = \ker(\theta)$. Since $K \triangleleft H$, it suffices to show that $K = H$. Plainly, $K \leq H$. Applying Lagrange's Theorem, the integer $m = |G : K| = |\theta(G)|$ divides $|G|$ and also divides the integer $p! = |\text{Sym}(L)|$. Therefore, $m = p$, in other words, $|K| = |H|$. We have shown that $K = H$, as required.

4: By Eisenstein's Criterion, the polynomial $f(X) = X^n - 2$ is irreducible over $\mathbb{Q}$. We can put $K = \mathbb{Q}[\alpha]$, where α is a root to $f(X)$. In other words, $K = \mathbb{Q}[X]/(f(X))$.

Comment: Recall, when we are applying Eisenstein's Criterion to a polynomial over a field of fractions, we are actually applying a corollary whose proof relies on Gauss' Lemma. But that application is routine, and mention of the implicit appeal to Gauss' Lemma is unnecessary.

5: Given any equality $(a + b\sqrt{3})(A + B\sqrt{3}) = (\alpha + \beta\sqrt{3})$ with $a, b, A, B, \alpha, \beta \in \mathbb{Q}$, then

$$\begin{aligned} \alpha^2 - 3\beta^2 &= (aA + 3bB)^2 - 3(aB + bA)^2 \\ &= a^2A^2 - 3a^2B^2 - 3b^2A^2 + 9b^2B^2 = (a^2 - 3b^2)(A^2 - 3B^2). \end{aligned}$$

So, defining a function $N : \mathbb{Q}[\sqrt{3}] \rightarrow \mathbb{Q}$ by $N(a + b\sqrt{3}) = a^2 - 3b^2$, we have $N(uv) = N(u)N(v)$ for all $u, v \in \mathbb{Q}[\sqrt{3}]$.

Now let $u, v \in \mathbb{Z}[\sqrt{3}]$ with $v \neq 0$. Write $u/v = x + y\sqrt{3}$ with $x, y \in \mathbb{Q}$. Let $X, Y \in \mathbb{Z}$ with $|x - X| \leq 1/2 \geq |y - Y|$. Let $q, r \in \mathbb{Z}[\sqrt{3}]$ such that $q = X + Y\sqrt{3}$ and $u = qv + r$. Then $r/v = u/v - q = x - X + (y - Y)\sqrt{3}$. Therefore,

$$N(r) = N(v) |(x - X)^2 - 3(y - Y)^2| \leq 3N(v)/4 < N(v).$$

We have shown that N restricts to a Euclidian norm on $\mathbb{Z}[\sqrt{3}]$.



Group Theory Reprise

2 January 2026, LJB

1: (25 marks.) Let n be a positive integer.

(a) Briefly explain how the conjugacy classes of the symmetric group S_n are parameterized by the integer partitions $n = n_1 + \dots + n_r$.

(b) Under what conditions on a partition $n_1 + \dots + n_r$ is the corresponding conjugacy class contained in the alternating group A_n ? Justify your answer.

(c) Which of the integer partitions of 6 correspond to conjugacy classes contained in A_6 ? For each of those partitions, how many associated conjugacy classes of A_6 are there? What is the number of conjugacy classes of A_6 ?

2: (25 marks.) The generalized quaternion group of order 16 is

$$Q_{16} = \langle x, y : x^8 = y^4 = 1, x^4 = y^2, yxy^{-1} = x^{-1} \rangle.$$

In the following question, clearly state your conclusions separately from your justifications. (You will lose marks if the reader has to trawl through your discussions to extract fragments of your conclusions.)

(a) Determine the conjugacy classes of Q_{16} . How many conjugacy classes are there?

(b) Determine the subgroups of Q_{16} . How many subgroups are there?

3: (25 marks.) Let $H \leq G$ be groups and suppose that G is the union of the conjugates of H .

(a) Show that, if G is finite, then $H = G$.

(b) For infinite G , give a counter-example to the conclusion of (a). (Hint: consider upper triangular matrices over a suitable field.)

4: (25 marks.) Let G be a finite simple group such that, for every positive integer m dividing $|G|$, there is a subgroup of G with order m . Show that G is abelian.

Solutions to Reprise

1: Part (a). Recall, a partition is a tuple of non-increasing positive integers whose terms sum to n . The partitions of $n_1 + \dots$ of n and the conjugacy classes $[g]$ of elements $g \in S_n$ are in a bijective correspondence whereby $n_1 + \dots \leftrightarrow [g]$ provided g is a product of mutually disjoint cycles that have lengths $n_1, \dots$.

Part (b). For a positive integer m , an m cycle in S_n belongs to A_n if and only if m is odd. Therefore, a partition $n_1 + \dots$ correspondes to a conjugacy class contained in A_n if and only if there are an even number of indices i such that n_i is odd.

Part (c). Recall, by the orbit-stabilizer equation, given $g \in A_n$, then the conjugacy class $[g]_{S_n}$ of g in S_n splits into 2 conjugacy classes of A_n if and only if $C_{A_n}(g) = C_{S_n}(g)$. Otherwise $[g]_{S_n} = [g]_{A_n}$. The partitions of 6 with the property in (b) are

$$5 + 1, \quad 4 + 2, \quad 3 + 3, \quad 3 + 1 + 1 + 1, \quad 2 + 2 + 1 + 1, \quad 1 + 1 + 1 + 1 + 1 + 1.$$

Among those, only $5 + 1$ satisfies the splitting condition. So A_6 has 7 conjugacy classes.

2: Part (a). We have $xy = yx^{-1}$. So every element of Q_{16} can be written uniquely in the form x^r or yx^r where $0 \leq r \leq 7$. We also have $xyx^{-1} = yx^{-2}$. It is now clear that the conjugacy classes in $\langle x \rangle$ are

$$[1] = \{1\}, \quad [x] = \{x, x^7\}, \quad [x^2] = \{x^2, x^6\}, \quad [x^3] = \{x^3, x^5\}, \quad [x^4] = \{x^4\}$$

and the other conjugacy classes are $[y] = y\langle x^2 \rangle$ and $[yx] = yx\langle x^2 \rangle$. Thus, Q_{16} has 7 conjugacy classes.

Part (b). The subgroups are:

- $\{1\}$ with order 1,
- $\langle x^4 \rangle$ with order 2,
- $\langle x^2 \rangle, \langle y \rangle, \langle yx \rangle, \langle yx^2 \rangle, \langle yx^3 \rangle$ with order 4,
- $\langle x \rangle, \langle y, x^2 \rangle, \langle yx, x^2 \rangle$ with order 8,
- Q_{16} with order 16.

To see this, note that the 4 subgroups of $\langle x \rangle$ are easy to classify, and all the other subgroups have the form $\langle yx^r, H \rangle$, where $H \leq \langle x \rangle$. Thus, the total number of subgroups is 11.

3: Part (a). We have $G = \bigcup_g {}^g H$ where g runs over representatives of the cosets of H in G . So $|G| \leq \sum_g |H|$. But the reverse inequality also holds, since the number of indices g is $|G|/|H|$. We deduce that the conjugates ${}^g H$ are mutually disjoint. But 1 belongs to each ${}^g H$. So the number of indices g must be 1, in other words, $H = G$.

Part (b). Let F be any algebraically closed field. Let n be any integer with $n \geq 2$. Let $G = \text{GL}_n(F)$ and let H be the subgroup consisting of the upper triangular matrices in G . A standard result in linear algebra asserts that, over an algebraically closed field, every square matrix is similar to an upper triangular matrix. So G is the union of the conjugates of H .

4: Let p be the smallest prime divisor of $|G|$. Let $H < G$ such that $|G|/|H| = p$. By considering the action of G on the set of left cosets of H on G , we see that shows G has a quotient group isomorphic to a non-trivial subgroup of S_p . Since G is simple, G embeds in S_p . By Lagrange's Theorem, $|G|$ divides $p!$. The hypothesis on p now implies that $|G| = p$ and $G \cong C_p$, which is abelian.



Final

29 December 2025, LJB

1: (25 marks.) Let $\mathcal{X}$ be a non-empty class of finite groups that is closed under isomorphism, subgroups, quotient groups and extension. Here, closure under extension means that, given finite groups $K \trianglelefteq G$ such that K and G/K are in $\mathcal{X}$, then G is in $\mathcal{X}$. Now let G be any finite group. Resolve each of the following with a proof or a counter-example:

(a) There always exists a unique normal subgroup $K \trianglelefteq G$ that is minimum, with respect to inclusion, subject to the condition that G/K is in $\mathcal{X}$.

(b) There always exists a unique subgroup $J \leq G$ that is maximum, with respect to inclusion, subject to the condition that J is in $\mathcal{X}$.

(c) There always exists a unique normal subgroup $I \trianglelefteq G$ that is maximum, with respect to inclusion, subject to the condition that I is in $\mathcal{X}$.

2: (15 marks.) For which primes p does there exist a field extension K of $\mathbb{Q}$ such that $|K : \mathbb{Q}| = p$ and the Galois group $\text{Gal}(K/\mathbb{Q})$ is trivial?

3: (40 marks.) Let L be the splitting field for $X^4 - X^2 - 1$ over $\mathbb{Q}$.

(a) Show that $|L : \mathbb{Q}| = 8$.

(b) Show that the complex conjugation element of $\text{Gal}(L/\mathbb{Q})$ is not in the centre.

(c) Using parts (a) and (b), determine $\text{Gal}(L/\mathbb{Q})$ up to isomorphism.

(d) How many fields J are there such that $J \leq L$ and the extension $J/\mathbb{Q}$ is Galois?

4: (10 marks.) By considering the Frobenius automorphism, show that the automorphism group of any finite field is cyclic.

5: (10 marks.) Let $\mathcal{C}$ be the category whose objects are arbitrary sets and whose morphisms are arbitrary surjections, with the usual composition operation. Show that any span in $\mathcal{C}$ has a pushout in $\mathcal{C}$.

Solutions to Final

1: Part (a). True. Let $\mathcal{N}$ be the set of normal subgroups K of G such that $G/K \in \mathcal{X}$. Note that $G \in \mathcal{N}$, hence $\mathcal{N} \neq \emptyset$. Given $K, K' \in \mathcal{N}$, then the homomorphism

$$G \ni g \mapsto (gK, gK') \in G/K \times G/K'$$

has kernel $K \cap K'$. So $\mathcal{N}$ is closed under intersection. The minimum element of $\mathcal{N}$ is the intersection of the elements of $\mathcal{N}$.

Part (b). False. We can take $\mathcal{X}$ to be the class of finite p -groups, for a prime p . Letting P be any non-trivial finite p -group and letting P act non-trivially on a finite group A , then $P \ltimes A$ has at least 2 Sylow p -subgroups.

Part (c). True. Let $\mathcal{M} = \{I : \mathcal{X} \ni I \trianglelefteq G\}$. Note that $1 \in \mathcal{M}$, so $\mathcal{M} \neq \emptyset$. Let $I, I' \in \mathcal{X}$. Then $II'/I \cong I'/(I \cap I') \in \mathcal{X}$. Since $\mathcal{X}$ is closed under extension, $II' \in \mathcal{X}$. So $\mathcal{M}$ is closed under join. The maximum element of $\mathcal{M}$ is the join of the elements of $\mathcal{M}$.

2: The primes satisfying the specified condition are precisely the odd primes. To see this, first note that, given a field extension K of $\mathbb{Q}$ with degree 2. then K is the splitting field of a degree 2 polynomial over $\mathbb{Q}$, hence $\text{Gal}(K/\mathbb{Q}) \cong C_2$. For the converse, suppose p is odd. By Eisenstein's Criterion, $X^p - 2$ is irreducible over $\mathbb{Q}$. So, letting α be the unique real p -th root of 2, then $|\mathbb{Q}[\alpha] : \mathbb{Q}| = p$. By the uniqueness of α , we have $\text{Gal}(\mathbb{Q}[\alpha] : \mathbb{Q}) = 1$.

3: Part (a). Let $\alpha = (1 + \sqrt{5})/2$ and $\mu = \sqrt{\alpha}$. Let $\beta = (1 - \sqrt{5})/2$ and let ν and ν^* be the complex conjugate square roots of β . Then $\mu, -\mu, \nu, \nu^*$ are the roots to $X^4 - X^2 - 1$. Let

$$K = \mathbb{Q}[\sqrt{5}] = \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] .$$

We have $L = K[\mu, \nu]$ and

$$|L : \mathbb{Q}| = |L : K[\mu]| \cdot |K[\mu] : K| \cdot |K : \mathbb{Q}| = 2 \cdot 2 \cdot 2 = 8 .$$

Part (b). Write $G = \text{Gal}(L/\mathbb{Q})$. Let σ denote the conjugation element of G and let τ be any element of G such that $\tau(\nu) = \mu$. Then $\tau\sigma(\nu) = \tau(\nu^*) \neq \mu = \sigma\tau(\nu)$. So $\sigma \notin Z(G)$.

Part (c). Since G is of order 8 and has a non-central involution, $G \cong D_8$.

Part (d). By the Fundamental Theorem of Galois Theory, the specified fields J are the fixed fields of the normal subgroups of D_8 . There are 1, 1, 3, 1 normal subgroups with orders 1, 2, 4, 8, respectively. So the number of such J is 6.

4: Every finite field has the form $\mathbb{F}_q$ where $|\mathbb{F}_q| = q = p^n$, with p prime and n a positive integer. Recall, the Frobenius automorphism ϕ of $\mathbb{F}_q$ is given by $\phi(x) = x^p$ for all $x \in \mathbb{F}_q$. By considering the case where x is a generator of the cyclic group $\mathbb{F}_q^\times$, we deduce that, given an integer m , then $\phi^m = 1$ if and only if n divides m . In other words, ϕ has order n . Letting G be the cyclic subgroup of $\text{Aut}(\mathbb{F}_q)$ generated by ϕ , then $|G| \cong C_n$.

Now $\mathbb{F}_q$ is the splitting field for $X^q - X$ over $\mathbb{F}_p$. So the field extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois. Therefore,

$$|\text{Aut}(\mathbb{F}_q)| = |\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = |\mathbb{F}_q : \mathbb{F}_p| = n .$$

We deduce that $G = \text{Aut}(\mathbb{F}_q)$. So $\text{Aut}(\mathbb{F}_q)$ is cyclic with order n .

5: Consider a span

$$A \xleftarrow{\alpha} S \xrightarrow{\beta} B$$

in $\mathcal{C}$. For convenience of notation, we may assume that A and B are disjoint. That allows us to identify $A \sqcup B = A \cup B$. We define $\equiv$ to be the equivalence relation on $A \sqcup B$ generated by the condition that $\alpha(s) = \beta(s)$ for all $s \in S$. Let T denote the set of equivalence classes $[z]$ of elements $z \in A \sqcup B$. Let $\mu : A \rightarrow T$ and $\nu : B \rightarrow T$ be the functions such that $\mu(a) = [a]$ and $\nu(b) = [b]$ for $a \in A$ and $b \in B$. If $z \in A$, then $\mu(z) = [z]$. If $z \in B$ then, since β is surjective, there exists $s \in S$ such that $\beta(s) = z$, whereupon $\mu(\alpha(s)) = [z]$. So μ is surjective. Similarly ν is surjective. Thus, we have a cospan

$$A \xrightarrow{\mu} T \xleftarrow{\nu} B$$

in $\mathcal{C}$. It is obvious that, in the category of sets and perforce in $\mathcal{C}$ too, this cospan is a pushout of the given span.