D-MATH | Algebra I+II | HS17
Prof. Marc Burger | | FS18
Prof. Emmanuel Kowalski

Solution of the Midterm

1. Let G be a group and H a subgroup of G.

a)	The index of H in G is a prime number.	**False.** For example, $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ of index 4.
b)	If H is abelian, then H is normal in G.	**False.** For example, consider $G = S_3$ and its abelian subgroup $H = \{\mathrm{id}, (1\,2)\}$. Then $(1\,3)(1\,2)(1\,3)^{-1} = (3\,2) \notin H$, so that H is not normal in G.
c)	If G is abelian, then H is normal in G.	**True.** For each $h \in H$ and $g \in G$, abelianity of G implies that $ghg^{-1} = hgg^{-1} = h \in H$.
d)	If H is abelian and the index of H in G is two, then G is abelian.	**False.** For example, consider $G = S_3$ and $H = A_3$.
e)	If G is simple, then either $H = G$ or $H = \{1\}$.	**False.** If G is simple, then it can still contain non-trivial proper subgroups, as long as they are not normal. For example, take A_5, which is simple as proven in class, but contains the subgroup $\langle (1\,2)(3\,4) \rangle = \{\mathrm{id}, (1\,2)(3\,4)\}$.

2. Let G be a group acting on a set X and H a subgroup of G.

a)	If the action of G is faithful, so is the action of H on X.	**True.** Faithfulness of the action means that the corresponding map $G \longrightarrow \mathrm{Aut}(X)$ is injective. Composing this map with the inclusion $H \longrightarrow G$ we obtain that the action of H on X, corresponding to the resulting injective map $H \longrightarrow \mathrm{Aut}(X)$, is faithful as well.
b)	If the action of G has no fixed point, so does the action of H on X.	**False.** Let $G = S_2$ act on $X = \{1, 2\}$ in the usual way and $H = \{\mathrm{id}\}$. While G has no fixed point, H fixes the whole $X \neq \varnothing$.
c)	If the action of G is transitive, so is the action of H on X.	**False.** The same example given in b) is a counterexample.
d)	For each $x \in X$, $\mathrm{Stab}_H(x) = \mathrm{Stab}_G(x) \cap H$.	**True.** It follows immediately by definition.
e)	Each H-orbit of X is contained in a G-orbit of X.	**True.** If $y \in X$ is in the H-orbit of x, then $y = h \cdot x$ for some $h \in H \subset G$, so that y is in the G-orbit of x. This implies that the H-orbit of x is contained in the G-orbit of x.

3.

a)	A_7 is simple.	**True.** We saw in class that A_n is simple for each $n \in \mathbb{N}_{\geq 5}$.
b)	Every permutation has a unique decomposition into a product of transpositions.	**False.** For example, $S_3 \ni \mathrm{id} = (1\,2)(1\,2) = (1\,3)(1\,3)$.
c)	One can write down $(1\,2\,3\,4\,5)$ as a product of exactly 5 transpositions.	**False.** $(1\,2\,3\,4\,5)$ has signature 1 (it is equal to $(1\,5)(1\,4)(1\,3)(1\,2)$), while a product of 5 transposition has signature -1.
d)	The action of S_n on $\{1, \dots, n\}$ is transitive and faithful.	**True.** By definition, a permutation acts trivially on each $j \in \{1, \dots, n\}$ if and only if it is the identity (*faithfulness*). Moreover, for each $i, j \in \{1, \dots, n\}$, the permutation $(i\,j)$ sends i to j (*transitivity*).
e)	The permutations $(1\,2\,3)(4\,5)$ and $(1\,5)(2\,3\,4)$ are conjugated in S_8.	**True.** The two permutations have the same cyclic type, which characterize a conjugacy class as seen in the lecture (the conjugacy class of the given permutations corresponds to the partition $8 = 1 + 1 + 1 + 2 + 3$).

4. Let A be a commutative ring and I an ideal of A.

a)	If $f, g \in A[X]$ have both degree 3, then $f \cdot g$ has degree 6.	**False.** For example, consider $A = \mathbb{Z}/4\mathbb{Z}$ and the polynomials $f = g = 2X^3 + 1$ of degree 3. Then $fg = 4X^6 + 4X^3 + 1 = 1$ has degree 0.
b)	If I is a maximal ideal, then A/I is an integral domain.	**True.** By definition, if I is maximal, then A/I is a field, which implies that it is an integral domain.
c)	If A is a UFD, then $A[X]$ is a PID.	**False.** For example, consider $A = \mathbb{Z}$. It is a UFD, but $\mathbb{Z}[X]$ is not a PID (see Assignment 4, Exercise 4(c)).
d)	If A is a PID, then A/I is a PID.	**False.** For example, consider $A = \mathbb{Z}$ and $I = 4\mathbb{Z}$. Since $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, it is not a PID.
e)	The set of polynomials in $A[X]$ whose coefficients lie in I is an ideal in $A[X]$.	**True.** Let J be the given subset $A[X]$ consisting of polynomials whose coefficients lie in I. Clearly, $0 \in J$. Moreover, for each $f = \sum_i a_i X^i, g = \sum_i b_i X^i \in J$ (meaning, $a_i, b_i \in I$ for each i) and $h = \sum_i c_i X^i \in R[X]$, we see that $f - g = \sum_i (a_i - b_i) X^i \in J$ because $a_i - b_i \in I$ for each i and that $fh = \sum_i (\sum_{k=0}^{i} a_k b_{i-k}) X^i$ because $a_k b_{i-k} \in I$ for each i and k and I is closed under the sum. This means that the axioms of ideal are all satisfied.

5. Let A and B be commutative rings and $f : A \longrightarrow B$ a ring homomorphism. Let I be an ideal in A and denote by $p : A \longrightarrow A/I$ the usual projection.

a)	If $\ker(f) \subset I$, then there exists a ring homomorphism $g : A/I \longrightarrow B$ such that $f = g \circ p$.	**False.** This would hold (by the First Isomorphism Theorem) if one replaced "$\ker(f) \subset I$" with "$\ker(f) \supset I$". As a counterexample of the given statement, consider $A = B = \mathbb{Z}$, $f = \mathrm{id}_{\mathbb{Z}}$ and $I = 2\mathbb{Z}$. There exists no ring homomorphism $g : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}$ (because $0 \longmapsto 0$ and $1 \longmapsto 1$ imply that $\mathbb{Z}/2\mathbb{Z} \ni 0 = 2 = 1 + 1 \longmapsto 1 + 1 = 2 \neq 0 \in \mathbb{Z}$ is a contradiction).
b)	If B is a field, then $A/\ker(f)$ is an integral domain.	**True.** Since B is a field, its subring $\mathrm{im}(f)$ is an integral domain. Then we can conclude by observing that there exists an isomorphism $g : A/\ker(f) \cong \mathrm{im}(f) \subset B$ by the First Isomorphism Theorem.
c)	If f is injective, then A is isomorphic to a subring of B.	**True.** If A is injective, then $\ker(f) = 0$ and the projection p is an isomorphism, so that $A \cong A/\ker(f)\mathrm{im}(f) \subset B$.
d)	For every $b \in B$, there exists a unique ring homomorphism $h : A[X] \longrightarrow B$ sending $X \longmapsto b$.	**False.** In order to obtain a unique h, by the characterization of morphisms from a polynomial ring given in class, one needs to specify the map on the coefficients as well (e.g., ask that $h(X) = b$ and $h\|_A = f$). As a counterexample of the given statement, consider $A = B = \mathbb{C}$, $b = 0$. Then there exists a unique ring homomorphism $h : \mathbb{C}[X] \longrightarrow \mathbb{C}$ sending $X \longmapsto 0$ and such that $h\|_{\mathbb{C}} = \mathrm{id}_{\mathbb{C}}$ (it is the evaluation at 0) and a unique ring homomorphism $h' : \mathbb{C}[X] \longrightarrow \mathbb{C}$ sending $X \longmapsto 0$ and such that $h'\|_{\mathbb{C}}$ is the complex conjugation. Clearly $h \neq h'$, because $h(i) = i \neq -i = h'(i)$.
e)	If $J \subset B$ is a prime ideal, then $f^{-1}(J)$ is a prime ideal in A.	**True.** Let $q : B \longrightarrow B/J$ be the natural projection. As J is a prime ideal, B/J is an integral domain. Then $\ker(q \circ f) = f^{-1}(J)$ and by the First Isomorphism Theorem there is an injection $A/(f^{-1}(J)) \longrightarrow B/J$. Hence $A/(f^{-1}(J))$ is an integral domain as well and $(f^{-1}(J))$ is a prime ideal in A.

6. Let $R = \mathbb{Z}/15\mathbb{Z}$.

a)	R contains precisely 2 prime ideals.	**True.** The ideals of R are the preimages under the projection $p : \mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ of the ideals of $\mathbb{Z}$ containing $15\mathbb{Z}$. Hence the ideals of R are $R = \mathbb{Z}/15\mathbb{Z}$, $3\mathbb{Z}/15\mathbb{Z}$, $5\mathbb{Z}/15\mathbb{Z}$, $15\mathbb{Z}/15\mathbb{Z} = 0$ among which $3\mathbb{Z}/15\mathbb{Z}$ and $5\mathbb{Z}/15\mathbb{Z}$ are seen to be prime (because the corresponding quotients of R are fields of 3 and 5 elements respectively), while R is not prime by definition and 0 does contains $3 \cdot 5$, but neither 3 nor 5.
b)	$R[X]$ is a PID.	**False.** $R[X]$ is not an integral domain (since $3 \cdot 5 = 0$), so it cannot be a PID.
c)	The ideal generated by X in $R[X]$ is maximal.	**False.** The given ideal (X) is the kernel of the evaluation map $R[X] \longrightarrow R$ at 0, which is clearly surjective. By the First Isomorphism Theorem, $R[X]/(X) \cong R$, which is not a field. Hence (X) is not maximal.
d)	$\mathrm{card}(R^\times) = 8$	**True.** The units of R are given by the classes $a + 15\mathbb{Z}$ such that $\gcd(a, 15) = 1$. Hence $R^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ contains eight elements.
e)	There exists precisely one ring homomorphism $R \longrightarrow \mathbb{Z}$.	**False.** A ring homomorphism $R \longrightarrow \mathbb{Z}$ would have to send $0 \longmapsto 0$, $1 \longmapsto 1$ and hence $0 = 15 \cdot 1 \longmapsto 15 \neq 0$. This implies that there is no ring homomorphism $R \longrightarrow \mathbb{Z}$.

7.

a)	A free $\mathbb{Z}$-module has no torsion.	**True.** A free $\mathbb{Z}$-module is isomorphic to $\mathbb{Z}^{(I)}$ where I is a set. But $\mathbb{Z}^{(I)}$ has no torsion: if $0 \neq x = (x_i)_{i \in I} \in \mathbb{Z}^{(I)}$, then $x_{i_0} \neq 0$ for some $i_0 \in I$, and if for $n \in \mathbb{Z} \setminus \{0\}$ we write $n \cdot x = (y_i)_{i \in I}$, we see that $y_{i_0} = n x_{i_0} \neq 0$, so that $n \cdot x \neq 0$.
b)	A free $\mathbb{Z}$-module is finitely generated.	**False.** The free module $\mathbb{Z}^{(\mathbb{Z})}$ is not finitely generated.
c)	There are, up to isomorphism, 3 different abelian groups of 18 elements.	**False.** By the classification of finitely generated modules over a PID, abelian groups (i.e., $\mathbb{Z}$-modules) of 18 elements are all isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus H$, where H is an abelian group of 9 elements. There are then two possibilities: either $H \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $H \cong \mathbb{Z}/9\mathbb{Z}$, which give a total of 2 non-isomorphic abelian groups of 18 elements.
d)	There are, up to isomorphism, 4 different abelian group of 100 elements.	**True.** Similarly as in c), abelian groups (i.e., $\mathbb{Z}$-modules) of 100 elements are all isomorphic to $H_2 \oplus H_5$, where H_2 is an abelian group of 2^2 elements and H_5 is an abelian group of 5^2 elements. There are then two possibilities for H_2 ($H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $H_2 \cong \mathbb{Z}/4\mathbb{Z}$) and two for H_5 ($H_5 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ or $H_5 \cong \mathbb{Z}/25\mathbb{Z}$), which give a total of $2 \cdot 2 = 4$ non-isomorphic abelian groups of 100 elements.
e)	The $\mathbb{Z}$-module $\mathbb{Q}$ is free.	**False.** See Assignment 13, Exercise 5 for an argument.

8. Let L/K be a field extension.

a)	If L/K is of finite degree, then it is algebraic.	**True.** This was seen in class: a field extension L/K is of finite degree if and only if it is algebraic and finitely generated.
b)	If $f \in K[T]$ has no roots in L, then it is irreducible in $K[T]$.	**False.** For example, let $L = K = \mathbb{Q}$ and $f = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}$. The polynomial f is clearly not irreducible, although it has no roots in $\mathbb{Q}$.
c)	If $\alpha \in L$ is algebraic, then $\deg(\mathrm{irr}(\alpha; K)) = [K(\alpha) : K]$.	**True.** This equality was seen in class.
d)	If $\alpha, \beta \in L$ are transcendental over K, then $\alpha + \beta$ is transcendental over K.	**False.** Let $K = \mathbb{Q}$, $L = \mathbb{C}$, $\alpha = \pi$ and $\beta = 2 - \pi$. As seen in class, π is transcendental over $\mathbb{Q}$. Then $\mathbb{Q}(\pi) = \mathbb{Q}(1 - \pi)$ is an extension of $\mathbb{Q}$ of infinite degree, so that β is transcendental over $\mathbb{Q}$ as well, whereas $\alpha + \beta = 2 \in \mathbb{Q}$ is not.
e)	If $\alpha \in L \setminus K$ and $\alpha^2 \in K$, then $\mathrm{irr}(\alpha; K) = X^2 - \alpha^2$.	**True.** The polynomial $X^2 - \alpha^2 \in K[X]$ has root α and is monic. It is irreducible, because otherwise it would have a linear factor in $K[X]$, that is, it would have a root in K, which would imply that $\alpha \in K$ (because the roots of $X^2 - \alpha^2$ in K are $\pm\alpha$) which contradicts our assumption. Hence $X^2 - \alpha^2$ is the minimal polynomial of α over K.

9.

a)	There exists a finite field with 250 elements.	**False.** The cardinality of a finite field is, as seen in class, a power of a prime number, but $250 = 2 \cdot 5^3$ is not a power of a prime.
b)	Any finite field with 81 elements has characteristic 3.	**True.** As seen in class, a field of $81 = 3^4$ elements is a field extension of $\mathbb{F}_3$. Since $\mathbb{F}_3$ has characteristic 3, this must be the case for each of its extensions.
c)	The polynomial $X^{120} - 1 \in \mathbb{F}_{11}[X]$ has 10 roots in $\mathbb{F}_{11}$.	**True.** Each element $x \in \mathbb{F}_{11}$ satisfies $x^{11} = x$, which implies that $x^{121} = (x^{11})^{11} = x^{11} = x$ for each $x \in \mathbb{F}_{11}$. For $x \neq 0$, we can divide by x to obtain $x^{120} - 1$. Hence all the 10 invertible (i.e., non-zero) elements of $\mathbb{F}_{11}$ are roots of $X^{120} - 1$, while clearly 0 is not.
d)	If E is a finite field and F/E is an algebraic field extension, then F is a finite field.	**False.** The algebraic closure $\overline{E}$ of E is an algebraic extension by definition, but it has infinite cardinality, because it contains subfields with cardinality equal to an arbitrarily high power of the characteristic of E.
e)	If E is a finite field with m elements and F/E is a finite field extension of E, then $\mathrm{card}(F)$ is a multiple of m.	**True.** The cardinality of F is $\mathrm{card}(E)^{\dim_E(F)} = m^{[F:E]}$, hence it a positive power of m. As such, it is a multiple of m.

10. Consider the polynomial $f = X^5 - 1 \in \mathbb{Q}[X]$. Let $K/\mathbb{Q}$ be the splitting field of f in $\mathbb{C}$.

a)	$K/\mathbb{Q}$ has degree divisible by 6.	**False.** Since the roots of $X^5 - 1$ are all powers of $e^{\frac{2\pi i}{5}}$, we know that $K = \mathbb{Q}(e^{\frac{2\pi i}{5}})$. Then $1 \leq [K : \mathbb{Q}] = [\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}] = \deg(\mathrm{irr}(e^{\frac{2\pi i}{5}}, \mathbb{Q}))$ $\leq \deg(X^5 - 1) = 5$, so that $[K : \mathbb{Q}]$ cannot be a multiple of 6.
b)	f is the minimal polynomial of $e^{\frac{2\pi i}{5}}$ over $\mathbb{Q}$.	**False.** The polynomial f has the root 1 in $\mathbb{Q}$, so in particular is not irreducible and it cannot be the minimal polynomial of $e^{\frac{2\pi i}{5}}$. In fact, $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$ and the minimal polynomial of $e^{\frac{2\pi i}{5}}$ over $\mathbb{Q}$ is $X^4 + X^3 + X^2 + X + 1$.
c)	$\cos(\frac{2\pi}{5}) \in K$	**True.** $\cos(\frac{2\pi}{5}) = \frac{1}{2}(e^{\frac{2\pi i}{5}} + e^{-\frac{2\pi i}{5}})$, and K contains $e^{\frac{2\pi i}{5}}$ and $e^{-\frac{2\pi i}{5}}$ since they are roots of $X^5 - 1$.
d)	Any field homomorphism $K \longrightarrow \mathbb{C}$ has image equal to K.	**True.** Such a field homomorphism has image inside K, since $\mathbb{Q}(e^{\frac{2\pi i}{5}}) = K$ by a) and $e^{\frac{2\pi i}{5}}$ must be mapped to a root of $X^5 - 1$. But a field homomorphism is always injective, so that the resulting $\mathbb{Q}$-linear map $K \longrightarrow K$ must then be an isomorphism because K is a finite dimensional $\mathbb{Q}$-vector space, meaning that the image is K.
e)	$\mathbb{Q}(e^{\frac{2\pi i}{5}}) = K$.	**True.** See part a).