Test exam solutions

1. (Groups)

1. (Result from the course) Prove that if H is a normal subgroup of a group G, there is a group structure on the set G/H of right H-cosets of G such that the projection map $\pi : G \to G/H$ is a homomorphism. Prove that a homomorphism $\varphi : G \to G_1$, where G_1 is another arbitrary group, can be expressed in the form $\varphi = \tilde{\varphi} \circ \pi$ for some homomorphism $\tilde{\varphi} : G/H \to G_1$ if and only if $\ker(\varphi) \supset H$.

   Solution. We define a group structure on G/H as follows: (1) the identity element is $1_{G/H} = H$, the H-coset of the identity element in G; (2) the inverse of a coset xH is $x^{-1}H$; (3) the product of two cosets xH and yH is xyH.

   Before checking that these data define a group structure, we must check that the inverse and product are well-defined: the cosets $x^{-1}H$ (resp. xyH) should be independent of the choice of x (resp. x and y) in their respective cosets. For the product (the inverse being similar), this means that if we replace x by xh_1 and y by yh_2, where h_1 and h_2 are in H, we should have $xyH = xh_1yh_2H$. This is indeed the case, because H is normal in G: we have $xh_1yh_2 = xy \cdot y^{-1}h_1yh_2 = xyh_3$ where $h_3 = yh_1y^{-1}h_2$ belongs to H, so $xh_1yh_2H = xyh_3H = xyH$.

   Once this is done, it is easy to check all axioms for a group. For instance, associativity follows from the definition of the product.

   $$(xH) \cdot ((yH)(zH)) = xyzH = (xHyH) \cdot zH.$$

   For the second part, suppose first that $\varphi = \tilde{\varphi} \circ \pi$. Then for $h \in H$, we obtain $\varphi(h) = \tilde{\varphi}(\pi(h)) = 1$ since $\pi(h) = 1$ in G/H. Conversely, assume that the kernel of φ contains H. We claim that a map $\tilde{\varphi} : G/H \longrightarrow G_1$ is well-defined by $\tilde{\varphi}(xH) = \varphi(x)$. Indeed, if we replace x by xh_1, where $h_1 \in H$, we obtain $\varphi(xh_1) = \varphi(x)$ since $h_1 \in \ker(\varphi)$. Now we have

   $$\varphi(x) = \tilde{\varphi}(xH) = \tilde{\varphi}(\pi(x))$$

   so $\varphi = \tilde{\varphi} \circ \pi$. Moreover, $\tilde{\varphi}$ is a homomorphism: we have

   $$\tilde{\varphi}(xHyH) = \tilde{\varphi}(xyH) = \varphi(xy) = \varphi(x)\varphi(y) = \tilde{\varphi}(xH)\tilde{\varphi}(yH).$$

2. Which of the following statements are true (justify with a proof, a reference to a result of the course, or a counterexample):

   A. Every finite abelian group is isomorphic to a direct product of cyclic groups.

   B. Every subgroup of an abelian group is solvable.

Please turn over!

C. If a group G acts on a set X, then the stabilizer of a point $x \in X$ is a normal subgroup of G.

Solution. (A) True, by the structure theorem of finitely generated abelian groups.

(B) True, since a subgroup of an abelian group is abelian, and an abelian groups is solvable.

(C) False in general; for instance, if $n \geq 3$, and S_n acts on $\{1, \ldots, n\}$ by $\sigma \cdot n = \sigma(n)$, then the stabilizer H of 1 is not normal: its conjugates are the stabilizers of other elements, and these are not equal (because $n \geq 3$).

3. Let G be a group, H a subgroup of G and $\xi \in G$ an element such that $\xi H \xi = H$. Prove that $\xi^2 \in H$ and that $\xi H \xi^{-1} = H$ (which means that ξ belongs to the normalizer of H in G). Conversely, prove that if $\eta \in G$ is some element such that $\eta^2 \in H$ and $\eta \in N_G(H)$, then $\eta H \eta = H$.

Solution. From $\xi H \xi = H$, taking the element 1 in H, we get $\xi^2 \in H$. Now we write

$$\xi H \xi^{-1} = \xi H \xi \xi^{-2} = H \xi^{-2} = H,$$

since ξ^{-2} also belongs to H.

Conversely, we have

$$\eta H \eta = \eta H \eta^2 \eta^{-1} = \eta H \eta^{-1} = H$$

if $\eta^2 \in H$ and η normalizes H.

2. (Rings)

1. (Result from the course) Prove that in a principal ideal domain A, every non-zero element has a unique factorization into irreducible elements.

Solution. Existence: by contradiction, let $x \in A$ be a non-zero element without factorization. Then x is not irreducible, so we can write $x = y_1 y_1'$ with neither y_1 nor y_1' being a unit. One of these at least has no factorization, since otherwise x would have one. We may assume that y_1 has no factorization. Then we have

$$xA \subset y_1 A$$

and $xA \neq y_1 A$, since y_1' is not a unit.

Again y_1 is not irreducible so $y_1 = y_2 y_2'$ for some non-units y_2 and y_2', one of which at least (say y_2) has no factorization. Iterating, we obtain in this manner an infinite sequence

$$xA \subset y_1 A \subset y_2 A \subset \cdots$$

where all inclusions are strict. Let I be the union of the principal ideals in this sequence. Then I is an ideal of A, as one checks using the fact that the union is increasing. Since A is a principal ideal domain, there exists $z \in A$ such that $I = zA$. Since $z \in A$, there exists a y_j such that $z \in y_j A$. But then $zA \subset y_j A \subset I = zA$, so that $z = u y_j$ for some unit $u \in A^\times$. This then contradicts the fact that $y_j A = zA$ is a proper subset of $y_{j+1} A$.

See next page!

Uniqueness: If there exists elements with two factorizations, let x be one with factorizations

$$x = u_1 p_1^{n_1} \cdots p_k^{n_k} = u_2 q_1^{m_1} \cdots q_l^{m_l},$$

with irreducible elements p_i and q_j and $n_i \geq 1$, $m_j \geq 1$, chosen so that the sum

$$\sum_i n_i + \sum_j m_j$$

is as small as possible.

Then p_1 divides the right-hand side, so (because A is a principal ideal domain) must divide one of the factors $q_j^{m_j}$, so $p_1 A$ must be equal to one of the $q_j A$. Dividing out by p_1, we obtain two factorizations with smaller sum of exponents, a contradiction.

2. State the structure theorem for finitely-generated modules over a principal ideal domain.

Solution. Let A be a principal ideal domain, M a finitely generated A-module.

(1) There exists an integer $n \geq 0$ and an isomorphism

$$M \xrightarrow{\sim} A^n \oplus M_{tors}$$

where

$$M_{tors} = \{m \in M \mid am = 0 \text{ for some } a \neq 0\}$$

is the torsion submodule of M.

(2) There exist $m \geq 0$ and irreducible elements $r_1, \ldots, r_m$, such that the ideals $r_i A$ are pairwise coprime, $M_{tors}(r_i) \neq 0$ and

$$M_{tors} = \bigoplus_{i=1}^{m} M_{tors}(r_i)$$

where we denote

$$N(r) = \{n \in N \mid r^k n = 0 \text{ for some } k \geq 0\}$$

the r-primary submodule of any A-module N, for any irreducible element $r \in A$.

(3) For each i, there exist $s_i \geq 1$ and a sequence

$$1 \leq \nu_{i,1} \leq \cdots \leq \nu_{i,s_i}$$

and an isomorphism

$$M_{tors}(r_i) = M(r_i) \xrightarrow{\sim} \bigoplus_{1 \leq j \leq s_i} A/r_i^{\nu_{i,j}} A.$$

3. Which of the following statements are true (justify with a proof, a reference to a result of the course, or a counterexample):

A. If I and J are ideals in a commutative ring A, then $A/(I \cap J)$ is isomorphic to $A/I \times A/J$.

Please turn over!

B. Any integral domain A is contained in a field K.

C. Any non-zero commutative ring contains a prime ideal.

D. If A is a commutative ring and $I \subset A$ is a prime ideal, then A/I is a field.

Solution. (A) False in general: for instance, take $I = J = 0$ if A is an integral domain (then A is not isomorphic to $A \times A$).

(B) True: one can take K to be the field of fractions of A.

(C) True: in fact, such a ring contains a maximal ideal, and a maximal ideal is also a prime ideal.

(D) False: A/I is an integral domain, but not necessarily a field; for instance, take $A = \mathbb{C}[X, Y]$ and $I = XA$; then $A/I \simeq \mathbb{C}[Y]$ is an integral domain, so I is a prime ideal, but not a field.

4. Let K be a field and $n \geq 2$ an integer. Let I_n denote the principal ideal generated by X^n in $K[X]$, and let $A_n = K[X]/I_n$. Compute the group $A_n^\times$ of units in A_n. Prove that A_n has a unique maximal ideal; which ideal is it?

Solution. Let $x \in A_n$ be the image of X. It is easy to see that any $y \in A_n$ can be written uniquely

$$A_n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

where the a_i are in K. We have then

$$A_n^\times = \{y \in A_n \mid y = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \text{ with } a_0 \neq 0\}.$$

Indeed, note that in writing y as above, we have $a_0 = P(0)$, where $P \in K[X]$ is any polynomial with image y. So if y is a unit, with $yz = 1$ for some $z \in A_n$, we get $1 = P(0)Q(0) = a_0 Q(0)$, where Q has image z. This means that a_0 is non-zero, and this gives the inclusion of the units of A_n in the right-hand side.

Conversely, if $a_0 \neq 0$, then we look for an inverse of y in the form

$$z = a_0^{-1} + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

The equations expressing the relation $yz = 1$ are linear equations for the coefficients $b_1, \ldots, b_{n-1}$, and one sees that they form a triangular system with non-zero diagonal coefficients. Hence there is a solution.

The unique maximal ideal of A_n is the principal ideal I generated by x. Indeed, we see that A_n/I is isomorphic to K by mapping y to a_0, so that I is a maximal ideal.

Furthermore, if J is any proper ideal, it is contained in I, so that I is the unique maximal ideal: otherwise, there would exist some element y in J with $a_0 \neq 0$ (since $a_0 = 0$ implies that y is a multiple of x), and then $y \in A_n^\times$ would show that $J = A_n$.

See next page!

3. (Fields)

1. (Result from the course) Prove that given a field K and a non-constant polynomial $P \in K[X]$, there exists an extension L/K and an element $x \in L$ such that $P(x) = 0$.

   Solution. Let $Q \in K[X]$ be an irreducible factor of P, which exists since it is not constant. We will find an extension L/K where Q has a root, and such a root will be by construction a root of P as well. We write

   $$Q = \sum_{i=0}^{d} a_i X^i$$

   for some $a_i \in K$.
   Consider $\tilde{L} = K[X]/QK[X]$ and $\tilde{x} \in \tilde{L}$ the image of X under the projection $\pi : K[X] \to L$. Then $\tilde{L}$ is a field, and $\tilde{Q}(\tilde{x}) = 0$, where

   $$\tilde{Q} = \sum_i \pi(a_i) X^i.$$

   Moreover, there is an homomorphism $K \to \tilde{L}$ by composing the injection of K in $K[X]$ and the projection. Since both rings are fields, this is an injective homomorphism, which we denote ι.
   The only issue is that $\tilde{L}$ is not literally an extension of K. One goes around this by defining L as the disjoint union of K and the complement in $\tilde{L}$ of the image of the injective homomorphism $K \longrightarrow \tilde{L}$. There is a bijection $f : \tilde{L} \to L$ by mapping $\iota(y) \in \tilde{L}$ to $y \in K \subset L$ for any $y \in K$, and mapping $y \in \tilde{L} - \iota(K)$ to $y \in L$. One then defines a field structure on L so that f is an isomorphism of fields, by "transport of structure". The image of $\tilde{x}$ in L under f is then a root of Q in L.

2. Which of the following statements are true (justify with a proof, a reference to a result of the course, or a counterexample):

   A. If L/K is a finite extension and L contains some element x for which the minimal polynomial $\mathrm{Irr}(x; K)$ of x is separable, then L/K is separable.

   B. If K is a finite field, then its order is a prime number.

   C. If K is a field and L_1, L_2 are algebraically closed fields containing K, then L_1 is isomorphic to L_2.

   Solution. (A) False, this condition should be true at least for elements x generating L over K.

   (B) False, the order is a power of a prime number.

   (C) False (fields which are algebraically closed and *algebraic over* K) are isomorphic: for instance the fields $\bar{\mathbb{Q}}$ of algebraic numbers and $\mathbb{C}$, which are both algebraically closed and contain $\mathbb{Q}$ are not isomorphic (one is countable, and the other not).

4. (Galois theory)

1. (Result from the course) Given a field K, a separable non-constant polynomial $P \in K[X]$ of degree $d \geq 1$ and a splitting field L/K of P, explain the construction of an injective homomorphism $\mathrm{Gal}(L/K) \to S_d$.

   Solution. Let $Z \subset L$ be the set of roots of P in L. By definition of a splitting field and of the Galois group $G = \mathrm{Gal}(L/K)$, we have an action of G on Z by $\sigma \cdot z = \sigma(z)$. This gives a homomorphism

   $$f : G \to S_Z.$$

   This is injective because if $f(\sigma) = 1$, then $\sigma(z) = z$ for all $z \in Z$, and since Z generates L over K by definition, this implies that σ is the identity.

   Now fix an enumeration of the roots $Z = \{z_1, \ldots, z_d\}$, where $d = \deg(P)$. This gives an isomorphism $S_Z \to S_d$, and by composing, an injective homomorphism $G \to S_d$

2. (Result from the course) State and sketch the proof of the classification of Kummer extensions for cyclic extensions of degree d over a field K containing the d-th roots of unity.

   Solution. For K of characteristic coprime to d containing μ_d, a finite extension L/K is Galois with Galois group isomorphic to $\mathbb{Z}/d\mathbb{Z}$ if and only if there exists $y \in L$ such that $L = K(y)$ and $y^d \in K^\times$, and if moreover $y^e \notin K$ for any divisor $e < d$ of d.[1]

   Step 1 ("If"). Let $z = y^d \in K^\times$. All the roots of the equation $X^d = z$ are of the form $x = \xi y$ with $\xi \in \mu_d \subset K$, so L/K is normal. The assumption also shows that L/K is also separable. Then the map

   $$\sigma \mapsto \frac{\sigma(y)}{y}$$

   is an injective homomorphism of its Galois group to $\mu_d \simeq \mathbb{Z}/d\mathbb{Z}$. It is surjective because otherwise the image would be a subgroup $a\mathbb{Z}/d\mathbb{Z}$ where a divides d and $a > 1$. But then $y^{d/a}$ would be in K by Galois-invariance.

   Step 2 ("Only if"). Let L/K be cyclic of degree d. Let ξ be a generator of μ_d and σ a generator of the Galois group of L/K. For some $t \in K$, the expression

   $$y = t + \xi^{-1}\sigma(t) + \cdots + \xi^{-(d-1)}\sigma^{d-1}(t)$$

   is non-zero and satisfies $\sigma(y) = \xi y$. From this it follows that $L = K(y)$ and $y^d \in K^\times$, and moreover that $y^e \notin K$ for $e \mid d$ and $e < d$ (because y^e is not Galois-invariant: $\sigma(y^e) = \xi^e y^e$, and $\xi^e \neq 1$ since ξ generates μ_d).

3. Which of the following statements are true (justify with a proof, a reference to a result of the course, or a counterexample):

   A. If L/K is a finite extension of finite fields, then L/K is a Galois extension.

[1] This last part was not in the course but it useful to get "if and only if".

See next page!

B. For any field K of characteristic 0, any $n \geq 2$, and $L = K(y)$ where $y^n = 2$, the extension L/K is a Galois extension.

C. Any radical extension has a solvable Galois group.

Solution. (A) True: result from the course.

(B) False: it may not be normal if $n \geq 3$, for instance $K = \mathbb{Q}$, $n = 3$.

(C) False: a radical extension might not be a Galois extension.

4. Let L/K be a finite Galois extension with Galois group G. Let G' denote the commutator subgroup $[G, G]$ generated by all commutators $xyx^{-1}y^{-1}$ in G. Show that $L^{G'}/K$ is a Galois extension with $\mathrm{Gal}(L^{G'}/K)$ abelian. Show that any Galois extension E/K with $E \subset L$ and $\mathrm{Gal}(E/K)$ abelian is contained in $L^{G'}$.

   Solution. We know that G' is a normal subgroup of G because

   $$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}],$$

   so by Galois theory, the extension $L^{G'}/K$ is indeed a Galois extension. Its Galois group is G/G', which is abelian.

   If $L/E/K$ is such that E/K is Galois with abelian Galois group, then the subgroup $H = \mathrm{Gal}(L/E)$ is normal with G/H abelian. It follows that $H \supset G'$ (because any commutator maps to 1 in G/H), and therefore by the Galois correspondance that $E \subset L^{G'}$.

5. Let K be a field of characteristic zero, and let $\bar{K}$ be an algebraic closure of K. Let x and y be elements of $\bar{K}$ such that $K(x)$ and $K(y)$ are solvable extensions. Prove that $K(x + y)$ is also solvable.

   Solution. We have $K(x+y) \subset K(x, y) = K(x)(y)$. Let L_1 (resp. L_2) be a radical extension of K acontaining $K(x)$ (resp. $K(y)$). Then $K(x)(y) \subset L_1(y) \subset L_1L_2$, where L_1L_2 is the extension generated by $L_1 \cup L_2$ in $\bar{K}$. But writing L_1 first, and then L_2, as obtained by adjoining successive roots of radical equations, we see that L_1L_2 is also a radical extension. Hence $K(x + y)$ is solvable.