Algebra II 2023 Final Solutions

True or False Questions

Answer 'T(rue)' or 'F(alse)'. (You don't have to give a reason, but it might get you half a point if you are wrong.)

	T or F	Comment/Reason
1		
2		
3		
4		
5		
6		
7		
8		
9		

1. Every algebraic extension of a field is a finite extension. F - other way round
2. $\mathbb{C}$ is the algebraic closure of $\mathbb{Q}$. F - $\mathbb{C}$ contains $\overline{\mathbb{Q}}$, but also elements that are transcendental over $\mathbb{Q}$.
3. The non-zero elements of every finite field form a cyclic group under multiplication. T - This was a theorem.
4. A group is solvable if and only if it has a composition series with simple factor groups. F - 'Abelian', not 'simple'
5. Every finite abelian group with p dividing its order has exactly one Sylow p subgroup. T
6. For α and β algebraic and conjugate over a field F there is always an F-isomorphism of $F(\alpha)$ to $F(\beta)$. T
7. Any algebraic closure of $\mathbb{Q}(\sqrt{2})$ is isomorphic to any algebraic closure of $\mathbb{Q}(\sqrt{5})$. T - They are both closures of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ and there are all isomorphic.
8. $\mathbb{Q}(\pi)$ is splitting over $\mathbb{Q}(\pi^2)$. T - It splits the irreducible $x^2 - \pi^2$.
9. Every finite extension of every field F is separable over F. F

Short Answers/Computations/Definitions

The following Definitions and Short Answer questions can be answered without work/explanation. (If you are unsure of your answer though, a short explanation might get part marks.)

1. Find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. $\boxed{\{1\}}$ They are the same field, as the $\text{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q})$ is $x^4 - 10x^2 + 1$, so $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ has dimension 4 over $\mathbb{Q}$.

2. How many primitive 10^{th} roots of unity are there in GF(23)? $\boxed{\text{None.}}$ 10 doesn't divide 22.

3. A series $H_0 < H_1 < H_2 < H_3$ (or in one case, the group H_3) is
   - *subnormal* if ______________________________
   - *normal* if ______________________________
   - *composition* if ______________________________
   - *principle* if ______________________________
   - *solvable* if ______________________________

   Damn guys! You should know the definitions! I know there are a lot, but... these classes are your job. This should be free marks.

4. How many different composition series are there of $\mathbb{Z}_{60}$. $\boxed{12}$ This is the number of orders we can compose the factor groups $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$, and $\mathbb{Z}_5$.

5. How many Sylow 5-subgroups can a group of order 55 have? $\boxed{1 \text{ or } 11}$

6. An extension $E > F$ of a field F is
   - *algebraic* if ______________________________
   - *splitting* if ______________________________
   - *separable* if ______________________________

7. A field is perfect if ______________________________. There was a theorem stating that the following fields are perfect:

   ____.

8. Give an example of algebraic extension $E \geq F$ that is separable but not splitting. (Give some justification for this.) The extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, where $\alpha = \sqrt[3]{2}$ is not splitting because the other roots of $f(x) = \text{irr}(\sqrt[3]{2}) = x^3 - 2$ are not in $\mathbb{R}$ so not in $\mathbb{Q}(\alpha)$. But the roots are distinct, so the extension is separable.

Problems

Do one of problems 1 and 2 and one of problems 3 and 4.

1. For a subgroup H of a group G show that the normaliser

$$N[H] = \{g \in G \mid gHg^{-1} = H\}$$

is a subgroup of G.

Solution

If a and b are in $N[H]$ then $abH(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H$ so $ab \in n[H]$ showing that it is **closed**. As $1H1^{-1} = 1H1 = H$, $N[H]$ contains the **unit**, and since for $g \in N[H]$ we have $g^{-1}Hg = g^{-1}gHg^{-1}g = H$ we have that $N[H]$ has **inverse**. So it is a subgroup of G.

2. Show that no group G of order 80 is simple.

Solution

We have $80 = 2^4 \cdot 5$, so by the Sylow theorems there are 1 or 16 Sylow 5 subgroups. If there is only 1 then it is normal, and so G is not simple, so we may assume there are 16 respectively. These 16 subgroups can only intersect in the unit element, so together they contain $16(5-1) = 64$ elements of order 5. This leaves only 16 elements for the Sylow 2-subgroups, and so, having size 16, there is only one of them. This group is then normal, and so G is not simple.

3. Let $E \geq F$ be an algebraic extension of fields. Give a definition/characterisation of $\{E : F\}$, $[E : F]$, and $G(E/F)$ (or $|G(E/F)|$) and place them, with a 'one or two line proof' (using results from class) for each inequality, in the following string:

$$\underline{\hspace{3cm}} \leq \underline{\hspace{3cm}} \leq \underline{\hspace{3cm}}.$$

Solution

- $G(E/F)$: the group of F-automorphisms of E,
- $\{E : F\}$: number of images of E under F-automorphisms of the algebraic closure $\overline{F}$ of F,
- $[E : F]$: the dimension of E as a vector field over F.

We have

$$|G(E/F)| \leq \{E : F\} \leq [E : F].$$

The first inequality is from the Isomorphism Extension Theorem– every F-automorphism of E extends to a F-automorphism of $\overline{F}$. The second uses the multiplicity of these values for intermediate extensions $E \geq K \geq F$, and for simple extensions $E = F(\alpha)$ comes from is because an F-isomorphism of $F(\alpha)$ is determined by the image of α, which must be a conjugate of α, so is at most the degree d of $\mathrm{irr}(\alpha, F)$, while $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis of $F(\alpha)$ over F, so $[F(\alpha) : F] = d$.

4. Show that if α and β are both separable over F then $\alpha \pm \beta, \alpha\beta$ and α/β if $\beta \neq 0$ are all separable over F.

Solution

Assume that α and β are separable. By definition, $F(\alpha)$ and $F(\beta)$ are separable over F. Thus, in particular, $\{F(\beta) : F\} = [F(\beta) : F]$ and so all roots of $\mathrm{irr}(\beta, F)$ are distinct (as the index counts the distinct roots, and the dimension is the degree of $\mathrm{irr}(\beta, F)$). But then all roots of $\mathrm{irr}(\beta, F(\alpha))$, which divides $\mathrm{irr}(\beta, F)$, are also distinct, so $F(\alpha, \beta)$ is separable over $F(\alpha)$, and so over F. We had a theorem saying that an extension is separable if and only if all elements of the extension are separable, so the elements $\alpha \pm \beta, \alpha\beta$, and α/β of $F(\alpha, \beta)$ are separable over F.

Proofs

Choose **TWO** of the following theorems and prove them. (You may use other theorems that do not make these trivial, but state the theorem that you are using.)

1. For any prime p and integer $n \geq 1$, there is a finite field of order p^n.

Solution

This is Theorem 33.1 of the notes.

2. (Second Isomorphism Theorem) Where H and N are subgroups of G and H is normal in G, $(HN)/N \cong H/(H \cap N)$.

Solution

Theorem 34.4 of notes.

3. If G is a group and p is a prime dividing $|G|$, then G has an element of order p.

Solution

Theorem 36.3 of text

4. Let S be a set of automorphisms of a field E. The set E_S of all $a \in E$ that are fixed by all σ in S is a subfield of E.

Solution

Theorem 48.11 of text.