MATH 6320 – MIDTERM

Your Name

- You have 80 minutes to do this exam.
- No calculators!
- For justifications, please use complete sentences and make sure to explain any steps which are questionable.
- Good luck!

Problem	Total Points	Score
1	20	
2	20	
3	20	
4	20	
5	20	
Total	100	

1. Short answer questions (2.5 points each).

(a) What does it mean for a field extension $F \subseteq K$ to be separable?

Solution: It means that every element of K is a root of a separable polynomial $f(x) \in F[x]$. Recall that a separable polynomial is one without multiple roots.

(b) Give an example of a separable field extension that is not Galois.

Solution: $\mathbb{Q} \subseteq \mathbb{Q}[2^{1/3}]$ works, as do many others.

(c) Let $K = \mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{C}$. What group is $\mathrm{Gal}(K/\mathbb{Q})$?

Solution: Obviously $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}[\sqrt{2}] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$. Since both $x^2 - 2$ and $x^2 + 1$ split completely in K, we see that $K/\mathbb{Q}$ is Galois and hence $G = \mathrm{Gal}(K/\mathbb{Q})$ has 4 elements. Note G cannot be cyclic since it has two distinct elements of order 2 (notably the map that sends $\sqrt{2} \to -\sqrt{2}$ and fixes i coming from $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$ and then also complex conjugation). Hence $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

(d) If $K \supseteq \mathbb{Q}$ is a Galois extension of degree 6, at most how many proper subfields can K have that are not equal to $\mathbb{Q}$?

Solution: There are two groups of order 6, the cyclic one which has 2 proper non-maximal subgroups and S_3 which has 3 subgroups of order 2 and 1 one subgroup of order 3, or in other words 4 subgroups. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 6, and the subfields of K are in bijection with the subgroups of G, there can be at most 4 proper non-trivial subgroups of K.

(e) Suppose $W \subseteq R$ is a multiplicative set, $M \to N$ is a map of R-modules and the induced map $W^{-1}M \to W^{-1}N$ is injective. Give an example to show that $M \to N$ need not be injective.

Solution: Let $M = \mathbb{Z}/4$ and $N = \mathbb{Z}/2$ with the map $M \to N$ the canonical surjection (it is not injective). But if we set $W = \{12, 4, 8, \ldots\}$ the $W^{-1}M = W^{-1}N = 0$ and the map between them is certainly injective.

(f) Compute $\mathrm{Hom}_{k[x]}(k[x]/\langle x \rangle, k[x])$.

Solution: Suppose $\phi \in \mathrm{Hom}_{k[x]}(k[x]/\langle x \rangle, k[x])$. We will show that $\phi = 0$ is the zero homomorphism. Then for any $\overline{f} \in k[x]/\langle x \rangle$, $x\phi(\overline{f}) = \phi(x\overline{f}) = \phi(0) = 0$. Hence $x\phi(f) = 0 \in k[x]$. But $k[x]$ is an integral domain hence $\phi(f) = 0$. Thus ϕ is the zero homomorphism. In particular

$$\mathrm{Hom}_{k[x]}(k[x]/\langle x \rangle, k[x]) = 0.$$

(g) State one form of Nakayama's lemma.

Solution: Suppose $(R, \mathfrak{m})$ is a local ring and M is a finitely generated R-module. Suppose $\mathfrak{m}M = 0$ then $M = 0$.

(h) Suppose $I, J \subseteq R$ are ideals. If $I + J = R$ prove that $(R/I) \otimes_R (R/J) = 0$.

Solution: Write $1 = i + j \in I + J$. Then for any $\overline{a} \otimes \overline{b} \in (R/I) \otimes_R (R/J)$ we see that

$$\overline{a} \otimes \overline{b} = (\overline{a}1) \otimes \overline{b} = (\overline{a}i + \overline{a}j) \otimes \overline{b} = (\overline{a}i) \otimes \overline{b} + (\overline{a}j) \otimes \overline{b} = 0 \otimes \overline{b} + \overline{a} \otimes (j\overline{b}) = 0 \otimes \overline{b} + \overline{a} \otimes 0 = 0.$$

The result follows.

2. **(a)** Suppose that $f : R \to S$ is a map of rings. Show that the induced map $f^\sharp : \mathrm{Spec}S \to \mathrm{Spec}R$ is continuous in the Zariski topology. (12 points)

Solution: Choose $V(I) \subseteq \mathrm{Spec}R$ an arbitrary closed set. We will show that $(f^\sharp)^{-1}(V(I)) = V(IS)$ showing that the inverse image of a closed set is closed.

Suppose $Q \in (f^\sharp)^{-1}(V(I))$, then $f^\sharp(Q) = f^{-1}(Q) \in V(I)$. Hence $f^{-1}(Q) \supseteq I$ and so $f(I) \subseteq Q$ and hence $IS \subseteq Q$.

Conversely, suppose $P \in V(IS) \subseteq \mathrm{Spec}S$ so $IS \subseteq P$. Then $f^\sharp(P) = f^{-1}(P) \supseteq I$ and so $f^\sharp(P) \in V(I)$ as desired.

(b) If $S = R/I$ and $f : R \to S$ is the canonical surjection, show that $f^\sharp : \mathrm{Spec}S \to \mathrm{Spec}R$ is injective and show that the Zariski topology on $\mathrm{Spec}S$ is the same as the subspace topology induced by the injection $f^\sharp$. (8 points)

Solution: The primes of S are in bijection with the primes of R that contain I. This bijection is the map from (a) (ie, $f^\sharp$ is inverse image of a prime, which is how the bijection works as well). It follows that $f^\sharp$ is injective.

More generally, the ideals of S are in bijection with the ideals of R that contain I. In particular, if $J/I = \overline{J} \subseteq S$ is an ideal of S corresponding to the closed set $V(\overline{J})$, then we claim that $(f^\sharp)^{-1}(V(J)) = V(\overline{J})$. But the primes of $V(J)$ are those elements of $\mathrm{Spec}R$ that contain $J \supseteq I$. These correspond to the primes of $\mathrm{Spec}S$ that contain J/I. We have just shown that $f^\sharp$ is closed, injective and continuous. Hence (b) follows.

Consider the following fact.

Fact: Suppose K is a field and $K \subseteq L$ is an extension of fields (possibly infinite with tons of transcendental elements). Say $a_1, \ldots, a_n \in L$. If $K[a_1, \ldots, a_n]$ is a field, then each a_i is algebraic over K. [1]

3. Using the fact, show that if $k = \overline{k}$, then every single maximal ideal of $R = k[x_1, \ldots, x_n]$ is equal to $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ for some $\alpha_i \in k$. (20 points)

Solution: Obviously $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ is maximal in R for any $\alpha_i \in k$.
Now conversely suppose that $\mathfrak{m} \subseteq R$ is a maximal ideal. Consider the map $\phi : R \to R/\mathfrak{m}$. Obviously $k \subseteq R/\mathfrak{m}$ and by the fact, $k = R/\mathfrak{m}$. Set $\alpha_i = \phi(x_i) \in k$. Then certainly $x_i - \alpha_i \in \ker \phi = \mathfrak{m}$ for each i so $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle \subseteq \mathfrak{m}$. But both ideals are maximal, so this inclusion is equality. This completes the proof.

[1] There are various ways to prove this fact. If you want to convince yourself its true without a real proof, consider what would happen if a_1 was transcendental, then you'd need $\frac{1}{a_1}$, $\frac{1}{a_1+1}$, and more generally $\frac{1}{p(a_1)}$ where $p(a_1) \in R$ is some irreducible element. There's no way we can add all these to $K[a_1, \ldots, a_n]$ and keep it a finitely generated ring extension.

4. Suppose $K \subseteq L$ are fields. Suppose that $L = K[a]$ with $a \neq 0$. Suppose that $a^n \in K$ and that n is the smallest integer > 0 with this property.

(a) If $a^m \in K$ show that $n|m$. (4 points)

Solution: Write $m = qn + r$ with $n > r \geq 0$. Then $a^n, a^m \in K$ and so $a^r \in K$. Since n is the minimal integer with this property, $r = 0$ and (a) follows.

(b) Suppose that $K \subseteq L$ is separable. Show that $\mathrm{char}K \not| \ n$. (6 points)

Solution: Suppose that $p = \mathrm{char}K$ does divide n, $n = pm$. Since $a^n = (a^m)^p \in L$, and L/K is separable, we see that $a^m \in L$. This contradicts the choice of n.

(c) Now suppose that every root of unity in L also is an element of K. Show that $[L : K] = n$. (10 points)

Hint: If $p(x)$ is the minimal polynomial for a over K, then it divides $x^n - a^n$. Consider the constant term of $p(x)$ and extract an nth root of unity from part of it.

Solution: Note $p(x) | \prod_{i=0}^{n}(x - \zeta_n^i a)$ where ζ_n is a primitive nth root of unity. Then $p(x)$ is a product of terms $(x - \zeta_n^i a)$. It follows that $p(0) = a^d(\prod_j \zeta_n^{i_j}) \in L$ where d is the degree of $p(x)$. Since $p(0), a^d \in L$, we have $(\prod_j \zeta_n^{i_j}) \in L$, but this is a root of unity so $(\prod_j \zeta_n^{i_j}) \in K$. But $p(0) \in K$ hence $a^d \in K$. The only way this can happen is if $d = n$ by our choice of n. Thus $p(x) = x^n - a^n$ and in particular $[L : K] = \deg p(x) = n$.

5. Show that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic. (20 points)

Solution: Consider the Frobenius map $F \in G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ defined by $F(a) = a^p$ obviously this fixes $\mathbb{F}_p$ (since everything does). We will show that the order of F in G is equal to n. Indeed, every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^n} - x$ and so clearly F^n, the automorphism which sends $a \mapsto a^{p^n}$, is the identity. Hence the order of F divides n. On the other hand if $F^m = \mathrm{id}$, then the automorphism which sends $a \mapsto a^{p^m}$ is the identity and so every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^m} - x$. But the only way this can happen is if $m = n$. Since $\mathrm{ord}F = n$ and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n = |G| = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$, we see that G is cyclic as desired.