MATH 6320 – FINAL

Your Name

- You have 2 hours 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	14	
2	14	
3	18	
4	18	
5	18	
6	18	
Total	100	

1. Short answer questions (2 points each).

(a) Give an example of a commutative ring with unity R and a multiplicative set $W \subseteq R$ such that the map $R \to W^{-1}R$ ($x \mapsto \frac{x}{1}$) is *not* injective.

Solution: There are lots of correct examples. For instance any multiplicative set W containing zero will work (as long as $R \neq \{0\}$). Here's another specific one, $R = \mathbb{Q}[x,y]/\langle xy \rangle$, $W = \{1, x, x^2, \dots, \}$. Then $y \mapsto \frac{y}{1} = \frac{xy}{x} = \frac{0}{x}$.

(b) Give an example of a non-separable extension of fields.

Solution: $\mathbb{F}_p(x^p) \subseteq \mathbb{F}_p(x)$.

(c) What does it mean for a group G to be solvable?

Solution: This means that there is a chain of subgroups $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$ such that each H_{i+1}/H_i is Abelian for $i = 0, \dots, n-1$.

(d) What does it mean that $\{f_1, \dots, f_n\}$ is a Gröbner basis for $I \subseteq k[x_1, \dots, x_r]$ with respect to a monomial order $>$?

Solution: It means that $I = \langle f_1, \dots, f_n \rangle$ and that $\text{in}_>(I) = \langle \text{in}_>(f_1), \dots, \text{in}_>(f_n) \rangle$

(e) If $R = k[x]$, what is $\text{Ext}^3(R/\langle x-1 \rangle, R^2 \oplus R/\langle x+1 \rangle)$?

Solution: $R/\langle x-1 \rangle$ has a very short projective resolution, namely $0 \to R \xrightarrow{\cdot(x-1)} R \to R/\langle x-1 \rangle$. It follows that only Ext^1 and Ext^0 could possibly be nonzero.

(f) True or false, if $M \to N$ is a surjective map of $k[x,y]$-modules and $B = k[x,y]/\langle y^2 - x^3 \rangle$, then $M \otimes B \to N \otimes B$ is surjective.

Solution: Yes, tensor is right exact.

(g) What is the definition of $\sqrt{I}$, the radical of I, where I is an ideal in a commutative ring R with unity.

Solution: $\sqrt{I} = \{r \in R \mid r^n \in I \text{for some } n > 0\}$.

2. Short answer questions (2 points each).

(h) What is the definition of a linear representation of a finite group G?

Solution: It is a group homomorphism $\phi : G \to \mathrm{GL}(V)$ where V is a vector space (over some field).

(i) True or false, $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$.

Solution: True, obviously $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, and $i \notin \mathbb{Q}(\sqrt{2})$. Hence $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| = 2$ as well. Thus $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 2 \cdot 2 = 4$.

(j) If K is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, how many proper subfields does K have?

Solution: 5. We have seen many times that the Galois group G is S_3. The proper subfields of K correspond to the *non-trivial* subgroups of G by the Galois correspondence. The non-trivial subgroups of S_3 are $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle(123)\rangle, G$. There are 5 (five) of them.

(k) True or false, every ideal of $k[x, y, z]$ has at most 3 generators.

Solution: False. Consider for instance $\langle x^2, xy, xz, y^2, yz, y^2\rangle$.

(l) If $0 \to L \to M \to N \to 0$ is a split short exact sequence of R-modules, then is it always true that $0 \to \mathrm{Hom}_R(B, L) \to \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(B, N) \to 0$ is always also split exact?

Solution: Yes. If $N \to M$ is such that $N \to M \to N$ is the identity, then $\mathrm{Hom}(B, N) \to \mathrm{Hom}(B, M) \to \mathrm{Hom}(B, N)$ is also the identity.

(m) Give an example of an algebraic extension of fields which is not finite.

Solution: $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. Lots of other examples work too.

(n) Let K be the splitting field of $x^{p^n-1} - 1$ over $\mathbb{F}_p$. How many elements does K have?

Solution: The splitting field of $x^{p^n-1} - 1$ is the same as the splitting field of $x^{p^n} - x$. That has p^n elements, namely the elements of $\mathbb{F}_{p^n}$.

3. Suppose that $R = (\mathbb{Z}/2\mathbb{Z})[x,y]/\langle x^2+1, xy+1\rangle$. Explicitly list all the prime ideals of R. Is R an integral domain? (18 points)

Hint: You can mod out by the one equation before modding out by another. Modding out by $xy+1$ is inverting an element and so can be treated like inverting a certain multiplicative set.

Solution: Let $A = \mathbb{Z}/2\mathbb{Z}[x]$, let $W = \{1, x, x^2, \ldots\} \subseteq A$. From the hint, we see that $R \cong W^{-1}A/\langle x^2+1\rangle$ (since modding out by $xy+1$ first just makes $y := \frac{-1}{x}$). So the primes of R are in bijection with the primes of $W^{-1}A/\langle x^2+1\rangle$.

Hence the primes of R are in bijection with the primes of $A/\langle x^2+1\rangle$ that do not contain x by properties of localization. The primes of $A/\langle x^2+1\rangle$ are in bijection with the primes of A which contain $\langle x^2+1\rangle$. Fortunately, there is only one such prime. Note that $x^2+1 = (x+1)(x+1)$ (characteristic 2) and so the primes of $A/\langle x^2+1\rangle$ is simply $\Big\{(x+1)\big(A/\langle x^2+1\rangle\big)\Big\} = \Big\{\langle x+1\rangle_{A/\langle x^2+1\rangle}\Big\}$.

Now if we are inverting W, we ask does this prime contain x? Obviously it does not (since if $\langle x+1\rangle$ contains x, it contains $x+1-x=1$ which makes it non-prime). Hence there is exactly one prime ideal of $W^{-1}A/\langle x^2+1\rangle$, and hence there is exactly one prime in R, namely $\langle x+1\rangle_R$.

Finally we observe that R is not an integral domain since $(x+1)^2 = 0$ even though $x+1$ is not equal to zero.

4. Let F be a field of characteristic zero and let E/F be a finite Galois extension. Suppose that $E = F[\alpha]$. Show that $E \neq F[\alpha^2]$ if and only if there exists a $\sigma \in G = \mathrm{Gal}(E/F)$ with $\sigma(\alpha) = -\alpha$. (18 points)

Hint: If $E \neq F[\alpha^2]$ consider $\mathrm{Gal}(E/F[\alpha^2])$. Otherwise if σ exists, consider the field fixed by it.

Solution: Suppose first that $E \neq F[\alpha^2]$, then $F[\alpha^2] \subseteq E$ corresponds to a subgroup $H = \mathrm{Gal}(E, F[\alpha^2])$. Obviously $[E, F[\alpha^2]] \neq 1$ and α is a root of the polynomial $T^2 - \alpha$, so $[E, F[\alpha^2]] = 2$ and $\mathrm{Gal}(E/F[\alpha^2]) = \{1, \sigma\}$. Obviously σ must send α to another root of $T^2 - \alpha^2$, hence to $-\alpha$.

Conversely, suppose that there is an element $\sigma \in G$ with $\sigma(\alpha) = -\alpha$, then $\sigma^2 = 1$ and so setting $H = \langle\sigma\rangle$ we see that $|H| = 2$ and so E^H is a field with $[E : E^H] = |H| = 2$. Obviously α^2 is fixed by σ so $F[\alpha^2] \subseteq E^H$, but it's easy to see that $[E : F[\alpha^2]] \leq 2$ as well, since α is a root of the quadratic polynomialy $T^2 - \alpha^2$.

5. Suppose that $R = k[x, y]$ where k is a field. Let $I = \langle x, y \rangle$ be an ideal and notice we have an inclusion $0 \to I \to R$. Prove that the map $\mathrm{Hom}_R(R, R) \to \mathrm{Hom}_R(I, R)$ is an isomorphism. (18 points)

Hint: You may want to show that $\mathrm{Ext}^1(R/I, R) = 0$. You can do this directly with a free resolution, you basically have done this before in fact (there are other ways too, you can stick R/I into other short exact sequences).

Solution: We have a short exact sequence $0 \to I \to R \to R/I \to 0$ which induces a long exact sequence

$$0 \to \mathrm{Hom}(R/I, R) \to \mathrm{Hom}(R, R) \to \mathrm{Hom}(I, R) \to \mathrm{Ext}^1(R/I, R).$$

First we show that $\mathrm{Hom}(R/I, R) = 0$. Indeed, if $\phi : R/I \to R$ is an R-module homomorphism and $\phi(\overline{u}) = v \in R$ then $x\phi(\overline{u}) = \phi(\overline{ux}) = xv$. But $ux \in I$ so that $\overline{ux} = 0 \in R/I$. Hence $xv = 0$. But R is an integral domain so that $v = 0$. Hence ϕ is the zero homomorphism.

Next we show that $\mathrm{Ext}^1(R/I, R) = 0$. We can do it directy via a projective resolution:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & R & \xrightarrow{\begin{bmatrix} y \\ -x \end{bmatrix}} & R^2 & \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} & R & \xrightarrow{f \mapsto \overline{f}} & R/I & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \| & & \\
0 & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & R/I & \longrightarrow & 0
\end{array}$$

This is just like the projective resolution we did on that worksheet, just slightly longer. We apply $\mathrm{Hom}(\bullet, R)$ to the resolution part of the above and obtain $0 \to \mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R) \to \mathrm{Hom}(P_2, R) \to 0$. We need to compute $\mathrm{Ext}^1(R/I, R)$. By definition this is

$$\frac{\ker\big(\mathrm{Hom}(P_1, R) \to \mathrm{Hom}(P_2, R)\big)}{\mathrm{image}\big(\mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R)\big)}.$$

The only way to do this is to identify what these modules and the maps between them are. Fortunately, $\mathrm{Hom}(P_1, R) = R^2$ and $\mathrm{Hom}(P_0, R) = R = \mathrm{Hom}(P_2, R)$, so we need to figure out what the maps between them are. $R = \mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R) = R^2$ is the map which sends 1 to $\begin{bmatrix} x \\ y \end{bmatrix}$, represented by the matrix $\begin{bmatrix} x \\ y \end{bmatrix}$. $R^2 = \mathrm{Hom}(P_1, R) \to \mathrm{Hom}(P_2, R) = R$ is the map that sends $\begin{bmatrix} a \\ b \end{bmatrix}$ to $ay - bx$, represented by the matrix $\begin{bmatrix} y & -x \end{bmatrix}$. You can see these by working summand by summand and noting that $R \xrightarrow{\cdot f} R$ becomes $\mathrm{Hom}(R, R) \xrightarrow{\mathrm{Hom}(\cdot f, R)} \mathrm{Hom}(R, R)$ which is also identified with $\cdot f$.

Regardless, it is clear now that $\mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R) \to \mathrm{Hom}(P_2, R)$ is exact since it is, up to a sign, the same as our original resolution. But then $\mathrm{Ext}^1(R/I, R) = \frac{\ker\left(\mathrm{Hom}(P_1, R) \to \mathrm{Hom}(P_2, R)\right)}{\mathrm{image}\left(\mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R)\right)} = 0$ as claimed.

Now from our exact sequence we conclude that $0 \to \mathrm{Hom}(R, R) \to \mathrm{Hom}(I, R) \to 0$ is exact and hence $\mathrm{Hom}(R, R) \to \mathrm{Hom}(I, R)$ is an isomorphism as claimed.

6. Suppose that $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ is an extension of fields such that $F/\mathbb{Q}$ is finite and Galois with $G = \mathrm{Gal}(F/\mathbb{Q})$ being an Abelian group. Suppose $\alpha = a + bi \in F$ and $1 = |\alpha| = \sqrt{a^2 + b^2}$.

(a) Show that if τ is complex conjugation, then $\tau(F) \subseteq F$ and hence that $\tau \in G$. (6 points)

Hint: F is the splitting field of some polynomial $g(x) \in \mathbb{Q}[x]$.

Solution: Using the hint, assume g and monic, we see that $\tau(g) = g$ since the coefficients of g are in $\mathbb{Q}$. Thus if $g(x) = \prod(x - \alpha_i)$ for some $\alpha_1, \ldots, \alpha_n \in F$ and hence τ permutes the α_i. But the α_i generate F over $\mathbb{Q}$ and so $\tau(F) \subseteq F$ as claimed.

(b) Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial for α over $\mathbb{Q}$. Suppose that β is any other root of f, prove that $|\beta| = 1$ as well. (12 points)

Hint: We know that $\beta = \sigma(\alpha)$ for some $\sigma \in G$. Use the fact that G is Abelian. Also recall that $|\beta|^2 = \beta\tau(\beta)$. (8 points)

Solution: $1 = \sigma(1) = \sigma(\alpha\tau(\alpha)) = \sigma(\alpha)\sigma(\tau(\alpha)) = \beta\tau(\sigma(\alpha)) = \beta\tau(\beta) = |\beta|^2$ as desired.