MA 521 – Final
Fall 2019

Time: 3 hours

1. Answer all questions in the spaces provided. If you run out of room for an answer, continue on the back of the page. There is also two blank pages at the end for scratch work or continued answers.
2. Unless stated otherwise, justify your answers to receive full credit. Your answers do not have to be in complete sentences, but they do need to be understandable.
3. No calculators, notes, or other outside assistance is allowed.

Name: ______________________________

Question	Points	Score
1	5	
2	5	
3	15	
4	10	
5	20	
6	20	
7	15	
8	15	
9	15	
Total:	120	

1. (5 points) Give the factorization of $493 = 17 \cdot 29$ into irreducible elements in $\mathbb{Z}[i]$ and use it to write 493 as a sum of two integer squares in two different ways.

2. (5 points) Give an example of an integral domain that is not a principal ideal domain. (Justify your answer.)

3. Let $\varphi : G \to G'$ be a group homomorphism with $H \trianglelefteq G$ and $H' \trianglelefteq G'$.

   (a) (5 points) Show that $\varphi^{-1}(H')$ is a normal subgroup of G.

   (b) (5 points) Show that $\varphi(H)$ is a subgroup of G'.

   (c) (5 points) Give an example to show that $\varphi(H)$ need not be a normal in G'.

4. Let $I \subset \mathbb{R}[x]$ be the principal ideal generated by $(x-1)(x-2)$.

   (a) (5 points) List the ideals of $\mathbb{R}[x]/I$. Do not justify your answers.

   (b) (5 points) Give an explicit ring isomorphism $\varphi : \mathbb{R}[x]/I \to \mathbb{R}^2$ and its inverse $\varphi^{-1} : \mathbb{R}^2 \to \mathbb{R}[x]/I$, where $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is a ring under coordinate-wise addition and multiplication. Do not justify your answers.

5. Let R denote the ring of rational numbers of the form $R = \left\{ \dfrac{m}{5^n} : m, n \in \mathbb{Z} \right\}$. Let $\varphi : R \to \mathbb{Z}/4\mathbb{Z}$ be given by $\varphi(\frac{m}{5^n}) = \overline{m}$, where $\overline{m} = m + 4\mathbb{Z}$ is the image of m in $\mathbb{Z}/4\mathbb{Z}$.

   (a) (5 points) Which of the follow describe R. Circle all the apply.

   (A) an integral domain (B) a principal ideal domain (C) a field

   (D) an ideal of $\mathbb{Q}$ (E) a subring of $\mathbb{Q}$

   (b) (5 points) Show that φ is well-defined.

   (c) (5 points) Show that φ is a ring homomorphism.

   (d) (5 points) Let I be the kernel of φ. Is I a maximal ideal in R? If it is, explain why. If not, give a proper ideal J that strictly contains I.

6. Consider the field $K = \mathbb{F}_2[x]/\langle x^4+x+1\rangle$. Here you may take for granted that x^4+x+1 is irreducible in $\mathbb{F}_2[x]$.

   (a) (5 points) What is $[K : \mathbb{F}_2]$?

   (b) (5 points) Find the multiplicative inverse of x^2+1 in K.

   (c) (5 points) What are the possible orders of the elements in the group K^*? Give an example of each.

   (d) (5 points) What is the size of $\mathrm{Aut}(K/\mathbb{F}_2)$? Justify your answer.

7. Consider the fields $K = \mathbb{Q}(t_1, t_2, t_3, t_4)$ and $F = \mathbb{Q}(s_1, s_2, s_3, s_4)$, where t_1, t_2, t_3, t_4 are indeterminates and

$$s_1 = t_1 + t_2 + t_3 + t_4, \quad s_2 = \sum_{1 \le i < j \le 4} t_i t_j, \quad s_3 = \sum_{1 \le i < j < k \le 4} t_i t_j t_k, \quad \text{and} \quad s_4 = t_1 t_2 t_3 t_4.$$

(a) (5 points) What is the orbit of $\alpha = t_1 t_2 + t_3 t_4$ under $\mathrm{Aut}(K/F)$?

(b) (5 points) What is the minimal polynomial $m_{\alpha,F}(x)$ of α over F? (You may write it as a factored polynomial in $K[x]$.)

(c) (5 points) Is $F(\alpha)$ Galois over F?

8. True or false. Circle one. Do not justify your answers.

(a) (3 points) If a group G acts transitively on a set S, then $|S|$ divides G.

True False

(b) (3 points) For any subgroup $H \leq G$, the kernel of the action of G on the left cosets of H is a normal subgroup of G that is contained in H.

True False

(c) (3 points) If A, B are subgroups of the symmetric group S_5 with $|A| = |B| = 4$, then $A = \sigma B \sigma^{-1}$ for some $\sigma \in S_5$.

True False

(d) (3 points) If A and B are subgroups of a group G with $AB = G$ and $A \cap B = \{\text{id}\}$ then $G \cong A \times B$.

True False

(e) (3 points) Every group of order $493 = 17 \cdot 29$ is abelian.

True False

9. True or false. Circle one. Do not justify your answers.

(a) (3 points) The rings $\mathbb{Q}[x]/\langle x^2+2\rangle$ and $\mathbb{Q}[x]/\langle x^2\rangle$ are isomorphic.

True False

(b) (3 points) The derivative map $D_x : \mathbb{Q}[x] \to \mathbb{Q}[x]$ is a ring homomorphism.

True False

(c) (3 points) If K/F is a field extension, then F and K have the same characteristic.

True False

(d) (3 points) Every finite group is the Galois group of some field extension.

True False

(e) (3 points) If K is the splitting field of an irreducible, separable polynomial $f \in F[x]$, then $\mathrm{Aut}(K/F)$ acts transitively on the roots of f.

True False