Instructions: This exam has 12 pages. Students are allowed to use only the text book and notes from class and sessions. Students are not allowed to use any other resources, including other people, the internet or other text books. You must answer 10 out of the following 11 questions. No extra points will be rewarded. Place an “X” through the question you are not going to answer. Be sure to show all work for all problems. No credit will be given for answers without work shown. If you do not have enough room in the space provided you may use additional paper. Be sure to clearly label each problem and attach them to the exam.

Tests must be returned to Prof. C. Consani in Krieger Hall 410 B, on Thursday December 9 at 5:00pm.

Academic Honesty Certification

I certify that I have taken this exam with out the aid of unauthorized people or objects.

Signature: ___________________________ Date: ___________________________
1. (10 points)

(a)[6 points] Let $G$ be a group and let denote by $H$ and $K$ two subgroups of $G$. Show that:

\[ H \cup K \text{ is a subgroup of } G \iff \text{ either } H \subset K \text{ or } K \subset H. \]

Deduce from this fact that a group can never be the union of two proper subgroups.

(b)[4 points] Show that a group $G$ cannot be described as a product of two conjugate (to a same subgroup $H \leq G$) subgroups different from $G$.

**Sol.**

(a) We denote by $e$ the identity in $G$.

\[ \Rightarrow: \text{ If } H \cup K \text{ is a subgroup of } G, \text{ and if } H \text{ is not included in } K, \text{ then there exists } h \in H \setminus K \text{ (hence } h \neq e). \text{ Then, } \forall k \in K: \text{ } hk \in H \cup K \text{ (since } H \cup K \text{ is a subgroup). Hence it follows that } \forall k \in K, \text{ } hk \in H \text{ or } hk \in K. \text{ We discuss these two cases. If } hk \in K, \text{ then since } K \text{ is a subgroup of } G, \text{ } h = (hk)k^{-1} \in K \text{ and this contradicts the hypothesis. Therefore, one necessarily must assume } hk \in H \text{ and since } H \text{ is also a subgroup of } G, \text{ } k = h^{-1}(hk) \in H. \text{ This shows that } K \subset H. \]

\[ \Leftarrow: \text{ If } K \subset H, \text{ then } H \cup K = H \text{ and } H \cup K \text{ is therefore a subgroup of } G. \]

If $G$ were the union of two of its proper subgroups, then one of the two is contained in the other one and hence the largest one would coincide with $G$ and therefore it could not be a proper subgroup.

(b) We prove the contrapositive. One can easily reduce to the case that one of the conjugate subgroups of $H$ is $H$ itself (since multiplication by $G$ on $G$ from the right and from the left is a bijection). Thus, suppose $G = HgHg^{-1}$ for some $g \in G$. Then we have $G = Gg = HgHg^{-1}g = HgH$. Thus we must have $1 = hgh'$ for some $h, h' \in H$, and so $g = h^{-1}h'^{-1} \in H$. Hence $gHg^{-1} = H$, and so $G = H^2 = H$. 

2
2. (10 points) Consider the symmetric group $S_8$.

(a)[2 points] Write the permutation

$$
\sigma = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
7 & 5 & 8 & 6 & 2 & 4 & 3 & 1
\end{pmatrix}
$$

as a product of disjoint cycles.

(b)[2 points] Is it possible to write $\sigma$ as a product of 3-cycles? Give an explanation for your answer.

(c)[2 points] Find an element in $S_8$ that has maximal order. Call it $\tau$.

(d)[4 points] Let $H = \langle \sigma \rangle$ and $K = \langle \tau \rangle$ be the subgroups generated by $\sigma$ and $\tau$. Determine the cardinality of the set $HK = \{hk | h \in H, k \in K\}$. (Hint: Determine $H \cap K$ first.)

Sol. (a) $\sigma = (1738)(25)(46)$.

(b) No. $\sigma$ is an odd cycle. Products of 3-cycles are even.

(c) Any disjoint 5-cycle and 3-cycle gives the maximal order 15, e.g, $\tau = (12345)(678)$.

(d) Note that $|H| = 4$ and $|K| = 15$. So $\forall g \in H \cap K$, $g^4 = 1$ and $g^{15} = 1$. Therefore $g = (g^4)^4, (g^{15})^{-1} = 1$. So $H \cap K = \{1\}$. Now consider the map $\phi : H \times K \rightarrow HK$ where $(h,k) \mapsto hk$. Clearly $\phi$ is surjective. If $h_1k_1 = h_2k_2$, then $h_2^{-1}h_1 = g_2g_1^{-1} \in H \cap K = \{1\}$. So $h_1 = h_2$ and $k_1 = k_2$. Therefore $\phi$ is also 1-to-1. So $|HK| = |H| \cdot |K| = 60.$
Consider the group $\mathbb{Z}_{31}$ of integers mod. 31.

(a) [3 points] How many elements in $\mathbb{Z}_{31}$ do not have a square root?

(b) [2 points] Show that every element in $\mathbb{Z}_{31}$ has a unique 31-th root.

(c) [3 points] Show that the equation $x^2 \equiv -1 \pmod{31}$ has no integer solutions.

(d) [2 points] Does the group $\mathbb{Z}^*_31$ of invertible elements in $\mathbb{Z}_{31}$ contain a subgroup isomorphic to $\mathbb{Z}^*_22$? Explain your answer.

**Sol.**

(a) Note that 31 is a prime number. So the map $\varphi : \mathbb{Z}_{31} \to \mathbb{Z}_{31}$, $\varphi(a) = a^2$ is 2-to-1 on non-zero elements since $a^2 \equiv b^2 \iff (a-b)(a+b) \equiv 0 \pmod{31}$. Also $0^2 \equiv 0$. So there are $\frac{31-1}{2} + 1 = 16$ elements that have square roots. The other 15 do not.

(b) The map (Frobenius) $F : \mathbb{Z}_{31} \to \mathbb{Z}_{31}$, $F(a) = a^{31}$ is 1-to-1, because by Fermat’s theorem $a^{31} \equiv a$ for all $a$, so if $a^{31} \equiv b^{31}$ we get $a \equiv b$. Therefore $F$ is also surjective (why?), thus a bijection. So every element in $\mathbb{Z}_{31}$ has a unique 31-th root.

(c) If $x^{31} \equiv -1 \pmod{31}$, then $x \neq 0$ and $x^{30} \equiv (-1)^{15} \equiv -1 \pmod{31}$, but this contradicts Fermat’s theorem which states that $x^{30} \equiv 1$, $\forall x \neq 0$. So there cannot be any integer solution.

(d) We know that $|\mathbb{Z}^*_31| = 30$. Also $|\mathbb{Z}^*_22| = \varphi(22) = 10$. Both these groups are cyclic, thus since 10|30, we can conclude that there is a subgroup in $C_{30}$ that is isomorphic to $C_{10}$. We find elements of order 30 and 10, respectively. It is immediate to verify that 3 $\in\mathbb{Z}^*_31$ has order 30 and 7 $\in\mathbb{Z}^*_22$ has order 10.
4. (10 points) Let $G$ be a finite group and let $H$ be a subgroup of $G$ with index $[G : H] = 2$. Show that $H$ contains all the elements of $G$ of odd order.

**Sol.** Since $[G : H] = 2$ then $H$ is normal in $G$. Hence $G/H$ is a factor group. Let $x \in G$ have odd order $n$. Then

$$(xH)^n = x^n H = 1H = H,$$

and so the order of $xH$ divides $n$. In particular, the order of $xH$ is odd. But $G/H$ has order $[G : H] = 2$, and since the nontrivial element of $G/H$ has order 2 we must have $xH = H$, which shows that $x \in H$. 


5. (10 points) Let $F$ be a field and let $F[X]$ be the ring of polynomials with coefficients in $F$. Prove that there are infinitely many irreducible, monic polynomials in $F[X]$.

\textbf{Sol.} Assume there is only a finite number of irreducible polynomials, say $p_1(x), p_2(x), \ldots, p_n(x)$. Since in $F[X]$ the unique factorization holds, every irreducible element generates a prime ideal, so each $p_i(x)$ generates a prime ideal (i.e. they are prime elements). Now consider the monic polynomial $q(x) = \prod_{i=1}^{n} p_i(x) + 1$. By construction, $q(x)$ is not divisible by any of the $p_i(x)$, hence either it generates a prime ideal, or it is divisible by another prime element greater than $p_n(x)$, contradicting the assumption of a finite number of prime (irreducible) monic polynomials.
6. (10 points)

(a) [6 points] Let $p$ be a prime number. Show that $f(X) = X^p - pX - 1$ is irreducible in the polynomial ring $\mathbb{Q}[X]$.

(b) [4 points] Show that the polynomial $g(X) = X^4 + 5X^2 + 3X + 2$ is irreducible over the field of rational numbers.

Sol. (a) Since the Eisenstein’s Criterion does not directly apply to $f(X)$, we look at the image of $f(X)$ via the ring automorphism $\mathbb{Q}[X] \to \mathbb{Q}[X], 1 \mapsto 1, X \mapsto X + 1$. Then the image of $f(X)$ is $f(X + 1) = X^p + pX^{p-1} + \frac{p(p-1)}{2}X^p - \cdots + \frac{p(p-1)(p-2)}{2}X^3 + \frac{p(p-1)}{2}X^2 - p$, which is now irreducible by the Eisenstein’s Criterion, with the choice of the prime being $p$.

(b) The rational roots test applied to $g(X)$ gives us no roots of $g(X)$ in $\mathbb{Q}$, so there are no linear factors of $g(X)$ with coefficients in $\mathbb{Q}$, and then by comparing coefficients of the product of two degree 2 polynomials, we see that there are no degree 2 polynomials using which $g(X)$ could factor into, thus $g(X)$ is irreducible in $\mathbb{Q}[X]$. 
7. (10 points)

(a) [4 points] Find a factorization of the principal ideal generated by \(19 + 8i\) into prime ideals in the ring \(\mathbb{Z}[i]\) of Gaussian integers.

(b) [6 points] Assume to know that \(\mathbb{Z}[i]\) is a principal ideal domain. Describe the factor ring \(\mathbb{Z}[i]/(1 + 2i)\): is it a field? If yes, give an explicit description of this field.

Sol. (a) We compute the norm of \(19 + 8i\) in \(\mathbb{Z}\): \(N(19 + 8i) = 19^2 + 8^2 = 425 = 5^2 \cdot 17\). It follows from the multiplicativity of the norm that \(19 + 8i\) has three prime factors in \(\mathbb{Z}[i]\): two of norm 5 and one of norm 17. \(\pm 1 \pm 2i\) are the primes of norm 5, while \(\pm 1 \pm 4i\) are primes of norm 17. Trial and error yields a factorization of \(19 + 18i = (1 + 2i)^2(−1 − 4i)\) into primes.

(b) Note that \(N(1 + 2i) = 5\) and that \(5 = (1 + 2i)(1 − 2i)\) in \(\mathbb{Z}[i]\). Note also that \(1 + 2i\) is irreducible in \(\mathbb{Z}[i]\), otherwise 5 would properly factor in \(\mathbb{Z}\) (apply again the multiplicativity property of the Norm). Moreover, \((1 + 2i) = (2 − i)\) as principal ideals in \(\mathbb{Z}[i]\) (\(1 + 2i = i(2 − i)\), and \(i \in \mathbb{Z}[i]^*\)). Then, we obtain the isomorphisms \(\mathbb{Z}[i]/(1 + 2i) \cong \mathbb{Z}[i]/(2 − i) \cong \mathbb{Z}/5\mathbb{Z}\), by mapping \(\mathbb{Z}[i] \xrightarrow{\phi} \mathbb{Z}/5\mathbb{Z}\), \(1 \mapsto 1\) and \(i \mapsto 2\). Note that \(\text{Ker}(\phi) = (2 − i)\), since we know that \(\text{Ker}(\phi) = (a + bi)\), for some \(a, b \in \mathbb{Z}\) and that \(2 − i\) is an irreducible element in \(\mathbb{Z}[i]\) whose norm is a prime number.
8. (10 points)
   (a) [2 points] Consider the polynomial \( f(X) = X^2 + 2X + 3 \in \mathbb{Z}[X] \). Prove that \( f(X) \) is irreducible in \( \mathbb{Z}_5[X] \).

   (b) [4 points] Let \( F \) be the factor field \( \mathbb{Z}_5[X]/\langle f(X) \rangle \). Determine the order of \( \overline{X} \in F^* \).

   (c) [4 points] Find an element of order 3 in \( F^* \).

   **Sol.** (a) It is easy to check that \( f(X) \) has no roots in \( \mathbb{Z}_5 \), so since it has degree 2, it follows that \( f(X) \) is irreducible in \( \mathbb{Z}_5[X] \).

   (b) \( F \) is a field with 25 elements, so \( F^* \) is a (cyclic) group with 24 elements. We thus compute \( (\overline{X})^a \), as \( a \) runs among the divisors of 24: \( \overline{X} \neq 1; (\overline{X})^2 = 3\overline{X} + 2 \neq 1 \). Similarly, one checks that \( (\overline{X})^3, (\overline{X})^4, (\overline{X})^6, (\overline{X})^8, (\overline{X})^{12} \neq 1 \). So the order of \( \overline{X} \) in \( F^* \) is 24.

   (c) \( (\overline{X})^8 = 4\overline{X} + 1 \) has order 3 in \( F^* \).
9. (10 points) Give an example of each of the following statements, with proofs:

(a) An irreducible polynomial of degree 3 in $\mathbb{Z}[X]$.

(b) A non-commutative ring of characteristic $p$, for $p$ prime.

(c) A ring with exactly 6 invertible elements.

(d) An infinite, non-commutative ring with only finitely many ideals.

(e) An infinite, commutative ring with only finitely many ideals.

(f) A finite non-commutative ring.

(g) A non-zero prime ideal of a commutative ring that is not maximal.

(h) A commutative ring that has exactly one maximal ideal and is not a field.

(i) A commutative ring with exactly two maximal ideals.

(k) A field with exactly 49 elements

Sol. (a) There are many...for example $X^3 + X + 1$ (apply the rational root test).

(b) The ring $M_n(\mathbb{F}_p)$ of square $n \times n$ matrices with entries in $\mathbb{F}_p$.

(c) $\mathbb{Z}/7\mathbb{Z}$.

(d) Any infinite division ring is a good example, for instance the (field of) Real Hamilton Quaternions.

(e) Any infinite field.

(f) $M_n(\mathbb{F}_p)$, for $n \geq 2$.

(g) $(0) \subset \mathbb{Z}$.

(h) $\{ \frac{m}{n} \in \mathbb{Q} | m, n \in \mathbb{Z}; p \nmid n \}$, for some prime number $p$. The maximal ideal is $\{ \frac{m}{n} | m, n \in \mathbb{Z}; p \mid m, p \nmid n \}$

(j) The direct product of two copies of the ring as in (h).

(k) The factor ring of $\mathbb{F}_7[X]$ by any irreducible polynomial of degree 2 has $7^2 = 49$ elements.
10. (10 points) Let $R_1$ and $R_2$ be commutative rings with identities and let $R = R_1 \times R_2$.

(a) [4 points] Show that every ideal $I$ of $R$ is of the form $I = I_1 \times I_2$, with $I_i$ ideal of $R_i$ for $i = 1, 2$.

(b) [3 points] Find all prime ideals of $R$.

(c) [3 points] Find all maximal ideals of $R$. 

Sol. (a) Let $I$ be an ideal of $R$, and let $(a, b) \in I$. Then $(a, b) \cdot (1, 0) = (a, 0)$, and $(a, b) \cdot (0, 1) = (0, b)$, so $I = I_1 \times I_2$, where $I_1$ is the set of $x \in R_1$ such that $(x, y) \in I$ for some $y$. Similar for $I_2$. It is easy to show that these sets are ideals.

(b) Prime ideals are of the form $\wp_1 \times R_2$ or $R_1 \times \wp_2$, for prime ideals $\wp_1, \wp_2$ in $R_1, R_2$ respectively.

(c) Maximal ideals are prime ideals in a commutative ring, so similar answer as in part (b), with $\wp_i$ replaced by $m_i$ maximal ideals in $R_i$. 

11. (10 points) A local ring $A$ is a commutative, unital ring with a unique maximal ideal.

Which of the following rings is local?

(a) [5 points] $A = \mathbb{Z}/p^r\mathbb{Z}$ (p prime number, $r \in \mathbb{N}$).

(b) [5 points] $A_1 = (\mathbb{Z}/p\mathbb{Z})[X]$ ring of polynomials in $X$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$.

For each ring, show or provide a counterexample to the statement: “the ring is local”.

Sol. We show that $A$ is local. The ideals of $A$ are obtained by projecting ideals of $\mathbb{Z}$ to $A$, using the natural projection map $\mathbb{Z} \to A$. Hence, the ideals of $A$ are generated by $\tilde{n} \in A$, for $0 \leq n \leq p^r - 1$. If $(n, p^r) = 1$, the ideal $\langle \tilde{n} \rangle \subset A$ is equal to $\langle 1 \rangle = A$. Hence the ideals of $A$ are $\langle \tilde{q}p \rangle$, with $0 \leq q \leq p^{r-1} - 1$. Moreover, $\langle \tilde{p} \rangle$ contains all other ideals of $A$ and $\langle \tilde{p} \rangle = p\mathbb{Z}/p^r\mathbb{Z}$. This is the only maximal ideal of $A$, which is therefore a local ring.

$A_1$ is not local: $\langle X \rangle$ and $\langle X - 1 \rangle$ are two maximal ideals in $A_1$ since $A_1/\langle X \rangle \cong \mathbb{Z}/p\mathbb{Z}$ a field (by sending $X \mapsto 0$) and $A_1/\langle X - 1 \rangle \cong \mathbb{Z}/p\mathbb{Z}$ (induced by sending $X \mapsto 1$). Here, one uses the fact that $A_1$ is UFD to factor a polynomial $p(X) \in A_1$ by $X$ or $X - 1$. Evidently $\langle X \rangle \neq \langle X - 1 \rangle$. 

12