Final Exam, Math 401
Monday, December 10

Problem 1. State a definition of:

1. Euler function (3 points);
2. a ring, a domain, a field (6 points);
3. an ideal, maximal ideal, prime ideal, principal ideal (8 points);
4. a UFD, PID, Euclidean domain (6 points);
5. irreducible elements and prime elements (4 points);
6. a group, subgroup, normal subgroup, $p-$group (8 points);
7. an action of a group G on a set X (5 points);
8. left cosets of a subgroup H of a group G and the factor group G/H (explain what are the elements of G/H and how the group structure is defined) (5 points).

Problem 2. State (5 points each)

1. Fermat's Little Theorem and Euler's Theorem;
2. Chinese Remainder Theorem;
3. Einsenstein Criterion;
4. Gauss Lemma;
5. division algorithm for polynomials;
6. First Isomorphism Theorem for groups and rings;
7. Lagrange's Theorem;
8. Sylow Theorem;

Problem 3. a) Using Euclid's algorithm compute $\gcd(2275, 462)$ and find $x, y \in \mathbb{Z}$ such that $\gcd(2275, 462) = x \cdot 2275 + y \cdot 462$ (check your answer) (8 points).

b) Compute $\phi(360)$. Explain the results you are using. (8 points)

c) Prove that if $\gcd(n, 21) = 1$ then $n^6 \equiv 1 \pmod{63}$. (10 points)

Problem 4. a) Find a greatest common divisor of the polynomials x^5+2 and $2x^4+x$ in $\mathbb{F}_5[x]$. Verify your answer.(5 points)

b) Factor each polynomial into irreducible factors. Justify you answer.

1. $2x^7 - 14x^3 + 49x - 35$ in $\mathbb{Q}[x]$ (5 points)
2. $x^3 + x^2 + x + 3$ in $\mathbb{F}_5[x]$ (5 points).
3. $x^4 + x^3 + x + 1$ in $\mathbb{F}_2[x]$ (5 points)

Problem 5. Let I and J be ideals of a ring R. Define $(I : J)$ as the set of all elements $r \in R$ such that $rj \in I$ for all $j \in J$, i.e.

$$(I : J) = \{r \in R : rj \in I \text{ for every } j \in J\}.$$

a) Prove that $(I : J)$ is an ideal of R. (8 points)

b) Prove that if I is a prime ideal then either $J \subseteq I$ or $(I : J) \subseteq I$ (8 points).

c) Suppose that R is a UFD and $a, b \in R - 0$. Show that $r \in (aR : bR)$ iff $a|rb$. Use it to prove that $(aR : bR) = \dfrac{a}{\gcd(a,b)}R$. (8 points)

Problem 6. In the group S_9 let $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 8 & 1 & 7 & 3 & 2 & 6 & 5 \end{pmatrix}$ and $b = (1,6,9)(2,7,8,3)$.

a) Are a and b conjugate? Explain your answer. (5 points)

b) Find $c \in S_9$ such that $cac^{-1} = a^{-1}$. (5 points)

c) Find $< a > \cap < b >$. (5 points)

d) Write b as a product of transpositions. (5 points)

Problem 7. a) Let G be a cyclic group and $f : G \longrightarrow G$ a function. Prove that f is a homomorphism iff there is an integer k such that $f(a) = a^k$ for every $a \in G$. (8 points)

b) Let G be a finite group with a normal subgroup N. Prove that if K is a subgroup of G such that $K \cap N = \{e\}$ then $|K|\,|[G : N]$. (8 points)

c) Let G be a finite group of order 231. Prove that G has a normal subgroup of order 7. (9 points)

** ***************

The following problems are optional. You may earn extra points, but work on these problems only after you are done with the other problems

Problem 8. Let P be a $p-$group.

a) Prove that any subgroup Q of index p in P is normal.

b) Prove that a proper subgroup B of P is contained in a subgroup A such that $[A : B] = p$. Hint: Use induction on $|P|$. Pick an element $a \in Z(P)$ of order p and consider two cases: $a \in B$ and $a \notin B$.

Problem 9. Prove that the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is an Euclidean domain with Euclidean function $f(a + b\sqrt{2}) = |a^2 - 2b^2|$.