Math 404 Final Exam Solutions

Short answer questions.

1. State the first isomorphism theorem (for rings, not groups).

   If $\varphi : R \to S$ is a surjective ring homomorphism with kernel I, then φ induces an isomorphism $\overline{\varphi} : R/I \cong S$.

2. Describe the Eisenstein criterion.

   Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with integer coefficients. If for some prime number p, p does not divide a_n, p does divide $a_{n-1}, \dots, a_0$, and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

3. Suppose that a real number α is constructible by straightedge and compass. What do you know about its irreducible polynomial? Give me a few examples of numbers which are constructible and numbers which are not (say, at least two examples of each sort).

   Its irreducible polynomial must have degree 2^k for some k. (This is not an "if and only if" condition, by the way—there are algebraic numbers with irreducible polynomials of degree 4 which are not constructible.) Some constructible numbers: 0, 1, $\frac{1}{2}$, $\sqrt{2}$. Some non-constructible numbers: $\sqrt[3]{2}$, π, e, $\cos 20°$.

Long answer questions.

4. Let F be a field. Consider this statement: a polynomial $g(x) \in F[x]$ is irreducible if and only if it has no roots. Is this always true, always false, or does it depend on the field? Justify your answer.

   As stated, this is false: over any field, every linear polynomial is irreducible, and every linear polynomial has a root. It might be reasonable to interpret the question as asking about polynomials of degree at least two. In this case, certainly if a polynomial has a root, it is not irreducible. The validity of the converse—if it has no roots, then it is irreducible—depends on the field. For example, it's true in $\mathbb{C}[x]$, because no polynomial of degree at least two is irreducible, and every polynomial of degree at least two has a root. It is false in $\mathbb{R}[x]$, though: $(x^2+1)^2$ has no roots in $\mathbb{R}$, but is not irreducible.

5. Is it possible to construct a regular 9-sided polygon with straightedge and compass? If so, describe a construction. If not, prove that it is impossible.

   It is impossible. If you could construct a regular 9-sided polygon with straightedge and compass, then you would have constructed a $40°$ angle. Since you can bisect any angle with straightedge and compass, then you could construct a $20°$ angle. But this is impossible—we know that $\cos 20°$ is not constructible.

6. Let R be a ring. Recall that an element p of R is *prime* if whenever p divides a product ab, then p divides one of the factors: either $p|a$ or $p|b$. An element q of R is *irreducible* if q can't be factored in any nontrivial way: if $q = rs$, then either r or s is a unit.

   (a) Let R be an integral domain, and prove that every prime element of R is irreducible.

   Let $p \in R$ be prime, and suppose $p = ab$. I want to show that either a or b must be a unit. Since $p = ab$, then $p|ab$, and since p is prime, I can conclude that either $p|a$ or $p|b$. Without loss of generality, suppose that $p|a$, say $a = pr$. Then $p = ab = (pr)b$. R is an integral domain, so I can cancel p from both sides: $1 = rb$. Thus b is a unit.

   (b) Let R be a principal ideal domain, and prove that every irreducible element of R is prime.

   Let $q \in R$ be irreducible, and suppose $q|ab$. I want to show that either $q|a$ or $q|b$. Since R is a principal ideal domain, it's probably a good idea to work with ideals. $q|ab$ is equivalent to $(ab) \subseteq (q)$. I want to show that either $(a) \subseteq (q)$ or $(b) \subseteq (q)$. Look at the ideal (a, q). This must be principal: $(a, q) = (r)$ for some $r \in R$, in which case q is a multiple of r: $q = rs$ for some s. Since q is irreducible, either r is an associate of q, or r is a unit. If r is an associate of q, then $(r) = (q)$, and since $a \in (r) = (q)$, I find that a is a multiple of q, as desired. On the other hand, if r is a unit, then $(a, q) = (r) = (1)$, so for some $u, v \in R$, $au + qv = 1$. Multiply both sides by b: $abu + qbv = b$. q divides both terms on the left-hand side, so q divides the right-hand side, as desired.

7. Prove that there are infinitely many primes congruent to 1 mod 4.

   Assume there are only finitely many primes congruent to 1 mod 4, say $p_1, p_2, \ldots, p_n$. Consider $N = (2p_1 \ldots p_n)^2 + 1$. This is not divisible by any of the p_i's, so it must have another prime factor, p. N is an odd number, so $p \neq 2$. Since p divides it, then if m is the term in parentheses, m is a root of $x^2 + 1$ mod p. This polynomial has roots mod p only when $p \equiv 1$ mod 4, so the prime factor is congruent to 1 mod 4, and it's not one of the ones we started with. So the original list was incomplete, so there must be infinitely many primes congruent to 1 mod 4.

Extra credit.

8. (a) For which of these fields F are there irreducible polynomials in $F[x]$ of every positive degree: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\ldots$, $\mathbb{F}_p$, $\ldots$? Prove that your answers are correct.

   Answer: $\mathbb{Q}$, $\mathbb{F}_p$ for all primes p.

   (b) Determine all positive integers which can be written as the sum of two squares (squares of integers, that is).

   Answer: all positive integers n whose prime factorization is of this form:

   $$n = p_1^{j_1} \cdots p_\ell^{j_\ell} (q_1^{k_1} \ldots q_m^{k_m})^2,$$

   where each prime p_i is either 2 or is congruent to 1 mod 4, and each prime q_i is congruent to 3 mod 4.