Part 1 of final exam review problems: problems from the first part of the course

1. These are essential. Expect to see one or more on the final.
   (a) State and prove the First Isomorphism Theorem for rings.
   (b) State and prove the Second Isomorphism Theorem for rings.
   (c) State and prove the Third Isomorphism Theorem for rings.

2. Let R be a commutative ring with 1 in the following. Let J be an ideal of R.
   (a) Complete the definition: J is a maximal ideal if
   (b) Complete the definition: J is a prime ideal if
   (c) Prove: J is a maximal if and only if R/J is a field. Provide a direct proof, i.e. show that J is maximal implies R/J has no proper, non-trivial ideal, and use this to prove that R/J is a field. Conversely, use that R/J is a field to show that the only proper ideal of R containing J is J itself.
   (d) Prove: If $R[x]$ is an integral domain, then R is an integral domain.
   (e) Prove: If R is a commutative ring with 1 and I is an ideal of R, then R/I is an integral domain if and only if R is a prime ideal.
   (f) Show that if A is an ideal and C is a subring, then $A + C$ is a subring of R. Show that if B, C are both subrings of R, it is not necessarily true that $B + C$ is a subring of R. Prove that if U and V are both ideals of R, then $U + V$ is an ideal of R. Show that if U is an ideal of R, and Y is a subring of R, then $U + Y$ is not necessarily an ideal of R.
   (g) Prove that if R is a PID, then for any increasing (i.e. ascending) infinite sequence of ideals $I_1 \subseteq I_2 \subseteq \ldots I_k \subseteq$, there exists $m \in \mathbb{N}$ such that $I_m = I_{m+n}$ for any $n \in \mathbb{N}$.
   (h) It is obvious that a finite ring contains maximal ideals, but this is not always the case for infinite rings. Prove that a commutative ring R with 1 contains a maximal ideal. (The crux of the argument—use that R has a 1 to show that the union of an ascending chain of *proper ideals* of R is also a proper ideal of R. Then apply Zorn's Lemma.)

3. Recall that if R is a ring, a *Euclidean norm* of R is a map $N : R \to \{0\} \cup \mathbb{N}$ that satisfies the following: For all $b \in R - \{0\}$, and all $a \in R$, there exist elements q and r in R satisfying $a = bq + r$, and either $N(b) > N(r)$ or $r = 0$. Prove that if R is a ring with Euclidean norm N, and $c \in R$ satisfies $N(c) = 0$, then $c = 0$ or c is a unit.

4. Prove that a Euclidean domain is a Principal Ideal Domain (PID).

5. Prove Gauss's Lemma: If $t(x) \in \mathbb{Z}$ is a monic polynomial, and $t(x)$ is irreducible in $\mathbb{Z}[x]$, then $t(x)$ is irreducible in $\mathbb{Q}[x]$. (Factor $t(x)$ in $\mathbb{Q}[x]$, clear out denominators, use a prime p involved in clearing out those denominators, and after reducing mod$p$ and working $\mathbb{Z}_p[x]$, do a cancellation—I strongly suggest reviewing this proof before the final.)

6. Provide the following two definitions, and do the proof of the last part.

   (a) An element $b \in R$ is **prime** if

   (b) An element $c \in R$ is **irreducible** if

   (c) Prove that if b is a prime element of R, then b is an irreducible element of R.

7. The Gaussian integers $R = \mathbb{Z}[i]$ have a Euclidean norm N given by $N(a + bi) = a^2 + b^2$. The norm N is **multiplicative**; that is, for all $\alpha, \beta \in R$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

   (a) Use the fact that N above is multiplicative to show that α is a unit of R implies that $N(\alpha) = 1$. What are the units of R?

   (b) Now show that if $\alpha \in R$ and $N(\alpha) = p$, where p is a prime number, then α is irreducible.

   (c) **No proof necessary.** Provide an irreducible $\gamma \in R$ such that γ is not a prime integer; then provide an irreducible $\phi \in R$ such that ϕ is a prime integer. Characterize the irreducibles of R.

8. You'll show $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain. Find two factorizations of $6 = \alpha\beta$, $6 = \gamma\phi$, and show that none of $\alpha, \beta, \gamma, \phi$ is a unit, that α is not an associate of either γ or ϕ, and that β is an associate of either γ or ϕ.

9. **Short answer.**

   (a) Provide a polynomial $b(x) = a_m x^m + \ldots + a_0 \in \mathbb{Z}[x]$ of degree $m > 1$ that is irreducible in $\mathbb{Q}[x]$ but is reducible in $\mathbb{Z}[x]$.

(b) Show that (x) is not a maximal ideal in $\mathbb{Z}[x]$ by providing an ideal I of $\mathbb{Z}[x]$ such that (x) is properly contained in I, and I is properly contained in $\mathbb{Z}[x]$.

(c) Provide a ring R, and ideals I and J of R, such that $(I \cap J) \neq IJ$.

10. True or false? If false, provide a specific counterexample.

    (a) In a Principal Ideal Domain (PID) R, every irreducible element of R is a prime element of R.

    (b) Let R be a commutative ring with 1. If R is a PID, then $R[x]$ is a PID.

    (c) If R is a PID, then R is a Unique Factorization Domain.

11. State (rigorously) Eisenstein's Criterion for irreducibility in $\mathbb{Z}[x]$.

12. Use Eisenstein's Criterion to show that if p is a prime number, then $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots x^1 + 1 (= \frac{x^p - 1}{x - 1})$ is irreducible in $\mathbb{Z}[x]$. [Note: Since $\Phi_p(x)$ is monic and irreducible over $\mathbb{Z}$, it is, by Gauss's Lemma, irreducible in $\mathbb{Q}[x]$.]

13. Let F be a field. Show that the non-commutative ring $M_2(F)$, the ring of two-by-two matrices over F, has no non-trivial proper ideal.

14. Use the Double-Extension Lemma for vector spaces to show that if K/F is a field extension and $[K : F] = p$ where p is a prime number, then for any $b \in K - F$, $F(b) = K$.

15. Prove that if K/F is a finite dimensional field extension, then every element of K is algebraic over F.