God created the integers; the rest is the work of man.
– Kronecker

No books or notes. You MUST OMIT ten points. Mark on your exam-book which 10 points (they can be parts of problems) are not being done. Maximum score: 100.

1. (15) Let $F = \mathbb{Z}_7[x]/(x^2 + x + 4)$.
   
   (a) (5) How many elements are in $F$?
   
   (b) (10) Find an explicit $\alpha \in F$ such that $\alpha \notin \mathbb{Z}_7$ and $\alpha^2 \in \mathbb{Z}_7$. Give $\alpha^2$ explicitly.

2. (20) Let $p$ be an integer prime of the form $p = 4k + 1$. (Note: You can assume earlier parts when working on later parts of this problem.)
   
   (a) (5) Show that there exists $a \in \mathbb{Z}_p^*$ with $a^2 = -1$ in $\mathbb{Z}_p$. (Hint: Let $g$ be a generator.)
   
   (b) (5) Let $a$ be a positive integer. Show that $a^2 + 1$ is not a prime in the Gaussian Integers.
   
   (c) (5) Using (2a,2b) show that $p$ is not a prime in the Gaussian Integers.
   
   (d) (5) Using (2c) show that there exist integers $x, y$ with $p = x^2 + y^2$.
   
   Note: This result is called the Fermat Two Squares Theorem.

3. (25) Let $R = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. You may assume, without proof, that $R$ is a ring. Set $d(\alpha) = |\alpha|^2$ where, as usual, $|x + iy| = \sqrt{x^2 + y^2}$.
   
   (a) (5) Draw a picture of the points of $R$ on the complex plane.
   
   (b) (5) Find all units of $R$ and prove they are the only units.
   
   (c) (5) State the conditions for $R$ to be a Euclidean Domain with size function $d$.
   
   (d) (10) Prove that $d$ does indeed satisfy those conditions.

4. (10) Let $F = \mathbb{Q}[x]/(x^2 - x - 1)$ Write each of $x^2, x^3, x^4, x^5$ in the form $a + bx$. 
5. (10) Let $\alpha$ be a complex number and assume $|Q(\alpha) : Q| = p$, with $p$ a prime number. Assume $\beta \in Q(\alpha)$ and $\beta \notin Q$. Prove that there exist $b_0, b_1, \ldots, b_{p-1} \in Q$ with $\alpha = b_0 + b_1\beta + \ldots + b_{p-1}\beta^{p-1}$.

6. (5) Use Eisenstein’s criteria to prove that $f(x) = x^{11} + 6x^8 + 12$ is irreducible in $\mathbb{Z}[x]$.

7. (10) Let $D$ be a P.I.D. Assume $\pi \in D$ is irreducible. Let $a \in D$. Prove that either $\pi|a$ or that there exist $x, y \in D$ with $x\pi + ya = 1$.

8. (5) Let $R = Q[x]/(x^3 - x - 1)$. Suppose that in $R$

$$ (1 + x)(a + bx + cx^2) = 1 $$

Give (but do not attempt to solve!!) a system of three linear equations in three unknowns that $a, b, c$ would satisfy.

9. (10) Let $Q = K_0 \subset K_1 \subset K_s$ be a tower of fields, all inside $C$, such that for each $1 \leq i \leq s$ either $K_i = K_{i-1}(\alpha_i)$ for some $\alpha_i$ with $\alpha_i^2 \in K_{i-1}$ or $K_i = K_{i-1}(\alpha_i)$ for some $\alpha_i$ with $\alpha_i^3 \in K_{i-1}$. Prove $2^{1/5} \notin K_s$.

The voyage of discovery lies not in seeking new horizons, but in seeking with new eyes.

– Proust