OLD ALGEBRA MIDTERM SOLUTIONS

1. (15) Let \( F = \mathbb{Z}_7[x]/(x^2 + x + 4) \). 
   \textit{Oooops:} On the actual exam we had 
   \( x^2 + x + 2 \) which does not give a field.

   (a) (5) How many elements are in \( F \)?
   \textbf{Solution:} 49, \( a + bx \) for \( a, b \in \mathbb{Z}_7 \).

   (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.
   \textbf{Solution:} As \( x^2 + x + 4 = 0 \) we complete the square, noting that \( \frac{1}{2} = 4 \), so that \( (x + 4)^2 = x^2 + x + 16 = 12 = 5 \) so \( \alpha = x + 4 \) and \( \alpha^2 = 5 \). (There are other solutions.)

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.)
   \textbf{Solution:} \( g^{4k} = 1 \). Set \( y = g^{2k} \). Then \( y^2 = 1 \) but \( y \neq 1 \) (as \( g \) is a generator) so \( y = -1 \). Take \( a = g^k \).

   (b) (5) Let \( a \) be a positive integer. Show that \( a^2 + 1 \) is not a prime in the Gaussian Integers.
   \textbf{Solution:} \( (a^2 + 1) = (a + i)(a - i) \). As \( a > 0 \) neither of the factors are units.

   (c) (5) Using (2a,2b) show that \( p \) is not a prime in the Gaussian Integers.
   \textbf{Solution:} Let \( a \) be from (2a). Then \( p | (a^2 + 1) \) but \( p \) divides neither of \( a + i, a - i \). But the Gaussian Integers are a Euclidean Domain in which primes \( \kappa \) must satisfy \( \kappa | \alpha \beta \Rightarrow \kappa | \alpha \lor \kappa | \beta \).

   (d) (5) Using (2c) show that there exist integers \( x, y \) with \( p = x^2 + y^2 \).
   \textbf{Note:} This result is called the Fermat Two Squares Theorem.
   \textbf{Solution:} As \( p \) is not prime some \( (x + iy)|p \). The size function \( d(\alpha) = |\alpha|^2 \) is multiplicative so \( x^2 + y^2 | d(p) = p^2 \). But \( d(x + iy) \) is neither one nor \( p^2 \) since the factorization is nontrivial so it must be \( p \).

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.
   \textbf{Solution:} It will be a rectangular lattice but in the \( Y \)-axis is it every \( \sqrt{2} \sim 1.4 \).
(b) (5) Find all units of $R$ and prove they are the only units.
Solution: The only units are $+1, -1$. As $d(\alpha)$ is multiplicative and a positive ($\alpha \neq 0$) integer a unit must have $d(\alpha) = 1$ so $x^2 + 2y^2 = 1$ which has only the solutions $y = 0, x = \pm 1$.

(c) (5) State the conditions for $R$ to be a Euclidean Domain with size function $d$.
Solution: First $d(\alpha)$ must always be a nonnegative integer. Then

i. $d(\alpha) \leq d(\alpha\beta)$
ii. For all $\alpha, \beta$ with $\beta \neq 0$ there exist $q, r$ with $\alpha = q\beta + r$ and either $r = 0$ or $d(r) < d(\beta)$.

(d) (10) Prove that $d$ does indeed satisfy those conditions.
Solution: Clearly $d(\alpha) \geq 1$ for all $\alpha$. (Note $d$ is not defined on zero.) As $d$ is multiplicative $d(\alpha\beta) = d(\alpha)d(\beta) \geq d(\alpha)$. For the second set $\alpha/\beta = x + y\sqrt{-2}$. Round off $x, y$ to the nearest integers $x_0, y_0$ and set $q = x_0 + y_0\sqrt{-2}$. Then

$$r = \alpha - q\beta = \beta((x - x_0) + (y - y_0)\sqrt{-2})$$

and

$$d(r) = |r|^2 = d(\beta)[(x - x_0)^2 + 2(y - y_0)^2] < d(\beta)$$

as the bracketed term is at most $3/4$. (One can also argue geometrically.)

4. (10) Let $F = Q[x]/(x^2 - x - 1)$ Write each of $x^2, x^3, x^4, x^5$ in the form $a + bx$
Solution: $x^2 = x + 1, x^3 = xx^2 = x^2 + x = 2x + 1, x^4 = xx^3 = 2x^2 + x = 3x + 2, x^5 = xx^4 = 3x^2 + 2x = 5x + 3$. (Fibonacci!)

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 $\alpha = b_0 + b_1\beta + \ldots + b_{p-1}\beta^{p-1}$.
Solution: As $\beta \in Q(\alpha), Q \subset Q(\beta) \subset Q(\alpha)$. As $\beta \notin Q, Q \neq Q(\beta)$. We showed in class, as a corollary of the tower theorem, that an extension of prime dimension has no strictly intermediate fields. Thus $Q(\beta) = Q(\alpha)$. Thus $\alpha \in Q(\beta)$ which means $\alpha$ can be written as desired above.

6. (5) Use Eisenstein’s criteria to prove that $f(x) = x^{11} + 6x^8 + 12$ is irreducible in $Z[x]$.
Solution: 3 divides the coefficients 12, 6 (and the zeroes) but does not divide the lead coefficient 1, while 9 = 3^2 does not divide the constant 12. (Note $p = 2$ does not work!)

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 $x\pi + ya = 1$.
Solution: Set $\alpha = \gcd(a, \pi)$. As $\alpha|\pi$, either $\alpha = 1$ or $\alpha = p$. If $\alpha = p$ then $p = \alpha|a$. If $\alpha = 1$ then, by the gcd property, we can write $\gcd(a, \pi) = xa + y\pi$ for some $x, y$, so $xa + y\pi = 1$. 
8. (5) Let $R = \mathbb{Q}(x^3 - x - 1)$. 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.

\textbf{Solution:} We multiply out

$$1 = (1+x)(a+bx+cx^2) = a + (a+b)x + (b+c)x^2 + cx^3 = a + (a+b)x + (b+c)x^2 + c(x+1)$$

Equating the constant term gives $a+c = 1$. The coefficients of $x, x^2$ must be zero so $a+b+c = 0$ and $b+c = 0$.

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 $2^{1/5} \notin K_s$.

\textbf{Solution:} All $[K_i : K_{i-1}] \leq 3$ so $[K_s : K_0]$ is the product of numbers at most 3 and so does not have a factor of 5. But $2^{1/5}$ satisfies $x^5 - 2 = 0$ which is irreducible by Eisenstein so if $2^{1/5} \in K_s$ then $Q \subset Q(2^{1/5}) \subset K_s$ so by the tower theorem $[Q(2^{1/5}) : Q] = 5[|K_s : Q|]$, a contradiction.