M2P4 Rings and Fields
Test 1, solutions.

1 February 2007

1. **4 marks**

(a) The invertible elements of $\mathbb{Z}/64$ are the residue classes of all odd numbers from 1 to 63. Indeed, if n is odd, then the highest common factor of n and 64 is 1. By Euclid's algorithm (see M1F) there are integers a and b such that $na + 64b = 1$, so that a is the inverse of n modulo 64.

If n is even, then mn is even for any $m \in \mathbb{Z}$, so that mn is never 1 modulo 64.

(b) **4 marks**

The zero divisors in $\mathbb{Z}/64$ are the residue classes of all even numbers from 2 to 62. Indeed, if n is even, $0 < n < 64$, then let 2^r, $r \geq 1$, be the highest power of 2 dividing n. Then $2^{8-r} < 64$ is not zero modulo 64, but $n2^{8-r}$ is zero modulo 64, so that n is a zero divisor.

2. **5 marks**

19 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Indeed, if $19 = (a+b\sqrt{-5})(c+d\sqrt{-5})$, then $19^2 = (a^2+5b^2)(c^2+5d^2)$. If $a^2+5b^2 = 1$ or $c^2+5d^2 = 1$, then one of the factors must be a unit. Otherwise we have $a^2+5b^2 = 19$, but this equation has no solutions in $\mathbb{Z}$ (clearly b^2 is at most 1).

3. **6 marks**

$\mathbb{Z}[\sqrt{-5}]$ is such an example. By Proposition 2.17 from lectures an irreducible element p dividing ab must divide a or b.

Now, 2 is irreducible, by the same argument as above: if $2 = (a + b\sqrt{-5})(c+d\sqrt{-5})$, then $2^2 = (a^2+5b^2)(c^2+5d^2)$. If $a^2+5b^2 = 1$ or $c^2+5d^2 = 1$, then one of the factors must be a unit. Otherwise we have $a^2+5b^2 = 2$, but this equation has no solutions in $\mathbb{Z}$.

On the other hand, 2 divides $6 = (1-\sqrt{-5})(1+\sqrt{-5})$, but 2 does not divide $1 \pm \sqrt{-5}$.

(Any other example is also fine.)