MA2215: Fields, rings, and modules
Homework problems due on November 12, 2012

1. (**a**) The quotient of $\mathbb{Z}[t]$ by the ideal generated by t^2+1 is manifestly isomorphic to $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is not a field, the ideal in question is not maximal.

(**b**) The quotient of $\mathbb{Z}[t]$ by the ideal generated by t and 2 is manifestly isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is a field, so the ideal is maximal.

2. The the quotient ring $\mathbb{Q}[t]/(t^2+1)\mathbb{Q}[t]$ is clearly isomorphic to $\mathbb{Q}[i]=\{x+yi\colon x,y\in\mathbb{Q}\}$. In the field of fractions of Gaussian integers, we have, for $(c,d)\neq(0,0)$, $\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{c^2+d^2}$, and that defines a homomorphism of that field into $\mathbb{Q}[i]$. That homomorphism is injective, since fields have no ideals that could be kernels of homomorphisms, and is surjective, since already the fractions $\frac{a+bi}{c}$ run over all of $\mathbb{Q}[i]$.

3. Let us assume that we have $a\neq 0$ such that ab is different from 1 for all b. Then among the elements ax, where x runs over R, there will be two equal elements, since the total number of elements is finite, and we skipped 1. Then $ax=ax'$, but for $a\neq 0$ and $x\neq x'$ that is impossible in an integral domain.

4. Since this field, considered just with addition as an operation, is a group of order 4, we may only have $1+1=0$ or $1+1+1+1=0$: the order of an element divides the order of the group by Lagrange's theorem. Also, $1+1+1+1=(1+1)(1+1)$, so if $1+1+1+1=0$, we must have $1+1=0$, because a field has no zero divisors.

5. We already proved that $1+1=0$. Let us take an element $a\neq 0,1$ in our field. The remaining fourth remaining element of the field is then $1+a$. Since we can multiply elements too, we should have $a^2=0$, or $a^2=1$, or $a^2=a$, or $a^2=1+a$. The first three assumptions would lead to zero divisors (since $a^2-1=(a-1)(a+1)=(a-1)^2$ and $a^2-a=a(a-1)$), so we have $a^2=1+a$, or $a^2+a+1=0$. Thus, we have a homomorphism from $\mathbb{F}_2[t]/(t^2+t+1)\mathbb{F}_2[t]$ to our field (that maps t to a), and this homomorphism is an isomorphism since it is surjective, and $\mathbb{F}_2[t]/(t^2+t+1)\mathbb{F}_2[t]$ is a field (because t^2+t+1 is irreducible) so the injectivity is automatic.

6. Indeed, looking at the additive group we conclude that $1+1+1=0$ but $1+1\neq 0$, so the natural map from $\mathbb{F}_3$ to our field that maps 1 to 1 is an isomorphism.

7. Since this field, considered just with addition as an operation, is a group of order 9, we may only have $1+1+1=0$ or $\underbrace{1+\ldots+1}_{9\text{ times}}=0$: the order of an element divides the order of the group by Lagrange's theorem. Also, $\underbrace{1+\ldots+1}_{9\text{ times}}=(1+1+1)(1+1+1)$, and the argument with zero divisors applies again.

8. We already proved that $1+1=0$. Let us take an element $a\neq 0,1$ in our field. Then the nine elements of the field are $0,\pm1,\pm a,\pm1\pm a$. Therefore a^2 is equal to one of these elements. From Assignment 4, we know irreducible quadratic polynomials over $\mathbb{F}_3$, which leads us to a conclusion that we can only have $a^2+a-1=0$, $a^2-a-1=0$, or $a^2+1=0$. (Otherwise, our field will have zero divisors.) In the latter case, we found root of -1 already. If $a^2\pm a-1=0$, we use the fact that $2=1+1=-1$ in our field, so $a^2\mp 2a-1=0$, therefore $(a\mp1)^2-2=0$, and $(a\mp1)^2+1=0$, and we have a square root of -1 again. Thus, we have a homomorphism from $\mathbb{F}_3[t]/(t^2+1)\mathbb{F}_3[t]$ to our field (that maps t to a or $a\pm1$ depending on which case we are considering), and this homomorphism is an isomorphism since it is surjective, and $\mathbb{F}_3[t]/(t^2+1)\mathbb{F}_3[t]$ is a field (because t^2+1 is irreducible) so the injectivity is automatic.