Solutions to Assignment 1

1. We need to check that the inverse of ~~any~~ ~~u∈G~~ $-u$ for any $u \in G$ is u. But $(-u)u = 1$, the identity of G so $-(-u) = u$.

2. Consider S, the set of 2×2 matrices over $\mathbb{R}$ with determinant > 1 with matrix multiplication as the operation. $(S, \cdot)$ is a semi-group and is not commutative. It is not a monoid because if ~~det~~ $AB = B$ for all (any) $B \in S$ then $\det(A) = 1$ so $A \notin S$.

3. a) Since K is a field, $(K,+)$ is an abelian group. We only need to check the axioms for scalars.

5) For $\lambda \in F$, $\mu, \xi \in K$, $\lambda(\mu + \xi) = \lambda\mu + \lambda\xi$ by distributivity in K.
6) For $\lambda, \mu \in F$, $\xi \in K$, $(\lambda\mu)\xi = \lambda(\mu\xi)$ by associativity in K.
7) For $\lambda, \mu \in F$, $\xi \in K$ $(\lambda + \mu)\xi = \lambda\xi + \mu\xi$ by distributivity in K.
8) $1 \in F$ and $1\xi = \xi$ for all $\xi \in K$.

b) The dimension of $\mathbb{Q}(i)$ as a $\mathbb{Q}$-vector space and $\mathbb{C}$ as a $\mathbb{R}$-vector space is 2 in both cases. A basis is $\{1, i\}$. No real multiple of 1 gives i so this set is linearly independent. $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ and $\mathbb{C} = \{a + bi : a, b \in \mathbb{C}\}$ so this is a spanning set as well.

If $\mathbb{R}$ was a finite-dim. $\mathbb{Q}$-vector space then as a $\mathbb{Q}$-vector space, $\mathbb{R} \cong \mathbb{Q}^n$ for some $n \in \mathbb{N}$. But there is no bijection between $\mathbb{R}$ and $\mathbb{Q}^n$. So $\mathbb{R}$ is infinite dimensional as a $\mathbb{Q}$-vector space.

4. x^2+x+1 is irreducible over $\mathbb{Z}_2$ since it has no solution in $\mathbb{Z}_2$.

Now $\mathbb{Z}_2[t]$ contains 4 elements: $0, 1, t$ and $1+t$.

The addition on $\mathbb{Z}_2[t]$ is isomorphic to that on $\mathbb{Z}_2 \times \mathbb{Z}_2$ as an abelian group so $(\mathbb{Z}_2[t], +)$ is an abelian group.

Looking at the definition of $\circ$, one sees that it is commutative and $1 = 1 + 0 \cdot t$ is the mult. identity and $0 \circ x = 0$ for any x.

So the only mult. we need to work out are $t \cdot t$, $t \cdot (1+t)$ and $(1+t) \circ (1+t)$.

$$t \cdot t = 1 + t, \quad t(1+t) = 1 \quad \text{and} \quad (1+t)(1+t) = t$$

We see then that every non-zero element has a mult. inverse and we only need to check associativity and distributivity:

For associativity, we want to see $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{Z}_2[t]$. If any one of a, b or c is 0 or 1 then this is clear. So we can assume $a, b, c \in \{t, 1+t\}$

In fact, with a little more work using commutativity one needs to check ~~2~~ calculations

$t(t(1+t)) = t$; $(tt)(1+t) = (1+t)(1+t)$
$= t$
and $t((1+t)(1+t)) = tt$; $(t(1+t))(1+t)$
$= (1+t)$. $= (1+t)$

So mult. is associative.

To see it is distributive, we need to check
$a(b+c) = ab+ac$. Again we can assume $a = t$ or $1+t$.

$b, c \in \{1, t, 1+t\}$, $b \neq c$ so there are 6 calculations:

a	b	c	
t	1	t	: $t(1+t) = 1$; $t + t\cdot t = t + 1 + t = 1$
t	1	$1+t$	: $t(t) = 1+t$; $t + t + t\cdot t = 1+t$
t	t	$1+t$	: $t(1) = t$; $t\cdot t + t(1+t) = 1+t+1 = t$
$1+t$	1	t	: $(1+t)(1+t) = t$; $1+t + (1+t)t = t$
$1+t$	1	$1+t$	: $(1+t)t = 1$; $1+t + (1+t)(1+t) = 1+t+t = 1$
$1+t$	t	$1+t$	: $(1+t)1 = 1+t$; $(1+t)t + (1+t)(1+t) = 1+t$.

So $\mathbb{Z}_2[t]$ satisfies distributivity. If we compute

$$t^2 + t + 1 = (1+t) + (t+1) = 0 \quad \text{in } \mathbb{Z}_2\{t\} \text{ so}$$

t satisfies $x^2 + x + 1$.