MATD01 Fields and Groups
Assignment 2
Solutions

1. We leave the verification that these are ideals to the reader. That $I \subset I + J$ is clear (write $a \in I$ as $a + 0$). To see $IJ \subset I \cap J$ note that for any $a \in I$ and $b \in J$, since I and J are ideals (and hence are closed under multiplication by arbitrary elements of R) we have $ab \in I \cap J$. Since I and J are closed under addition we get that every element of IJ belongs to $I \cap J$.

For an example where $IJ \subsetneq I \cap J$ take $R = \mathbb{Z}$, $I = J = (2)$. Then $IJ = (4)$ while $I \cap J = (2)$.

2. (a) Let $J \subset S$ be an ideal. Since $\phi(0) = 0 \in J$ we have $0 \in \phi^{-1}(J)$. Given $a, b \in \phi^{-1}(J)$, we have $\phi(a + b) = \phi(a) + \phi(b) \in J$ (as $\phi(a), \phi(b) \in J$ and J is a subgroup of S under addition). Thus $a + b \in \phi^{-1}(J)$. We have shown that $\phi^{-1}(J)$ is a subgroup of R under addition.

Now let $a \in \phi^{-1}(J)$ and $r \in R$. Then $\phi(ra) = \phi(r)\phi(a)$. Since $\phi(a) \in J$ and J is an ideal, it follows $\phi(ra) \in J$, i.e. $ra \in \phi^{-1}(J)$.

(b) Let $\phi : R \to S$ be a surjective ring homomorphism and I an ideal of R. We leave it to the reader to check that $\phi(I)$ is a subgroup under addition (you have seen this in your group theory course). Let $s \in \phi(I)$ and $t \in S$. Then there is $a \in I$ such that $\phi(a) = s$. Since ϕ is surjective, there is $r \in R$ such that $\phi(r) = t$. Since I is an ideal, $ar \in I$. We have $\phi(ar) = \phi(a)\phi(r) = st$, so that $st \in \phi(I)$.

(c) Let $\iota : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map (given by $\iota(n) = n$). Then $\mathbb{Z}$ is certainly an ideal of $\mathbb{Z}$ but $\iota(\mathbb{Z}) = \mathbb{Z}$ is not an ideal of $\mathbb{Q}$.

(d) Let $\pi : R \to R/I$ be the quotient map. Given an ideal $\mathcal{J} \subset R/I$, by Part (a) $\pi^{-1}(\mathcal{J})$ is an ideal of R. Moreover, since $0 \in \mathcal{J}$, we have $I = \ker(\pi) = \pi^{-1}(0) \subset \pi^{-1}(\mathcal{J})$. Define

$$\Gamma : \{\text{ideals of } R/I\} \to \{\text{ideals of } R \text{ that contain } I\}.$$

by $\Gamma(\mathcal{J}) = \pi^{-1}(\mathcal{J})$.

Given a ideal $J \subset R$, by (b) $\pi(J)$ is an ideal of R/I. Define

$$\Theta : \{\text{ideals of } R \text{ that contain } I\} \to \{\text{ideals of } R/I\}$$

by $\Theta(J) = \phi(I)$.

We claim that Γ and Θ are inverse functions. Indeed, that $\pi(\pi^{-1}(\mathcal{J})) = \mathcal{J}$ simply follows from surjectivity of π (check this). We now check that $\pi^{-1}(\pi(J)) = J$ for any ideal J of R with $I \subset J$. The inclusion $J \subset \pi^{-1}(\pi(J))$ is clear (why?). Let $a \in \pi^{-1}(\pi(J))$. Then $\pi(a) \in \pi(J)$, which is to say that $\pi(a) = \pi(b)$ for some $b \in J$. But then $a - b \in \ker(\pi) = I$. Since $I \subset J$, we have $a - b \in J$. Since $b \in J$ and J is a subgroup under addition, it follows that $a \in J$. Thus $\pi^{-1}(\pi(J)) \subset J$.

We leave it to the reader to check that Γ and Θ respect inclusions.

3. An ideal I of R is maximal if and only if there are exactly two ideals of R that contain I. The correspondence theorem implies that this is equivalent to R/I having exactly two ideals, which is equivalent to R/I being a field.

4. Let $I = (f(x))$. Suppose $f(x)$ is not irreducible. We show that $F[x]/(f(x))$ is not an integral domain. Indeed, if $f(x)$ is a unit, then $I = F[x]$ and $F[x]/I$ is not an integral domain (as it does not satisfy $1 \neq 0$). If $f(x)$ is not a unit, then being reducible it must factor as $f(x) = g(x)h(x)$ for some $g(x)$ and $h(x)$ of positive degree (and hence degree less than $\deg(f(x))$). Then in the quotient $F[x]/I$ we have $\overline{g(x)} \cdot \overline{h(x)} = \overline{f(x)} = 0$. But since $g(x)$ and $h(x)$ are nonzero and of degree less than the degree of $f(x)$, we have $\overline{g(x)}, \overline{h(x)} \neq 0$. (Being a nonzero multiple of $f(x)$, any nonzero element of I has degree $\geq \deg(f(x))$. Thus $g(x), h(x) \notin I$.)

5. Given $g(x)$, the division algorithm gives unique $q(x)$ and $r(x)$, the latter of degree less than $\deg(f(x))$, such that $g(x) = f(x)q(x) + r(x)$. Then $g(x) - r(x) \in (f(x))$, so that in the quotient $F[x]/(f(x))$ we have $\overline{g(x)} = \overline{r(x)}$.

As for uniqueness, if $\overline{r_1(x)} = \overline{r_2(x)}$ for $r_1(x)$ and $r_2(x)$ both of degree less than $\deg(f(x))$, then $r_1(x) - r_2(x)$ belongs to the ideal $(f(x))$ and has degree less than $\deg(f(x))$. It follows that $r_1(x) - r_2(x) = 0$.

6. (a) Let $\phi : \mathbb{Z} \to F$ be the canonical ring homomorphism. Then $\ker(\phi) = n\mathbb{Z}$ for some nonzero n, which we may assume to be nonnegative. Then n is simply the characteristic of F (why?). If $n = p$ is a prime number, then by the first isomorphism theorem ϕ induces an isomorphism $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Im}(\phi)$ (given by $\overline{a} \mapsto \phi(a)$). It follows that $\mathrm{Im}(\phi)$ is a subfield of F (why?). Since $\mathbb{Z}$ is cyclic (under addition) and generated by 1 and ϕ respects addition, $\mathrm{Im}(\phi)$ is generated under addition by $\phi(1) = 1_F$. Any subfield of F must contain 1_F and hence the additive subgroup generated by it, which is $\mathrm{Im}(\phi)$. Thus $\mathrm{Im}(\phi)$ is the prime field of F, completing the proof in the case that $\ker(\phi)$ is nonzero.

Now suppose $\ker(\phi) = 0$ (i.e. that ϕ is injective). We claim that ϕ extends to an injective ring map $\tilde{\phi} : \mathbb{Q} \to F$ (extends meaning that $\tilde{\phi} = \phi$ on $\mathbb{Z}$). For $m/n \in \mathbb{Q}$ with $m, n \in \mathbb{Z}$ and $n \neq 0$, define $\tilde{\phi}(m/n) = \phi(m)\phi(n)^{-1}$. To see that this makes sense first note that $\phi(n) \neq 0$ (and hence is a unit) since $\ker(\phi)$ is zero. Secondly, note that if $m/n = \ell/k$, then $mk = n\ell$, so that $\phi(m)\phi(k) = \phi(n)\phi(\ell)$. Since $\phi(n)$ and $\phi(k)$ are units it follows that $\phi(m)\phi(n)^{-1} = \phi(\ell)\phi(k)^{-1}$. (Why did we have to do the second check?)

We leave it to the reader to check that $\tilde{\phi}$ is a ring homomorphism and that it extends ϕ. Since $\mathbb{Q}$ is a field, $\tilde{\phi}$ is injective (alternatively you can find $\ker(\tilde{\phi})$). Being an injective ring homomorphism, $\tilde{\phi} : \mathbb{Q} \to F$ gives an isomorphism $\mathbb{Q} \simeq \mathrm{Im}(\tilde{\phi})$. We claim that $\mathrm{Im}(\tilde{\phi})$ is the prime field of F. Indeed, $\mathrm{Im}(\tilde{\phi})$ is certainly a subfield of F (why?). Any subfield of F contains 1_F, hence $\phi(m)$ for any integer m (why?), and hence $\phi(m)\phi(n)^{-1}$ for any $m, n \in \mathbb{Z}$, $n \neq 0$ (why?). Thus any subfield of F must contain $\mathrm{Im}(\tilde{\phi})$.

(b) Let F_0 be the prime field of F. Recalling the definition of a vector space we can see that F is a vector space over any subfield of F, and in particular over F_0. Being a finite set, F is finite dimensional as a vector space over F_0. Now if $\alpha_1, \ldots \alpha_n$ is a basis of F over F_0, then every element of F can be uniquely expressed as a linear combination $\sum_{i=1}^{n} c_i \alpha_i$ for some $c_i \in F_0$ $(1 \leq i \leq n)$. Thus $|F| = |F_0|^n = p^n$.

(c) Recall the following corollary of Lagrange's theorem from group theory: if G is a finite group, then $g^{|G|} = e$ for every $g \in G$. Applying this to the group $F^\times$ we see that for every nonzero $x \in F$ we have $x^{q-1} = 1$, or equivalently $x^q - x = 0$. The latter equation is trivially satisfied by 0 as well.

7. (a) Suppose the polynomial x^2+1 has a root α in F. Then x^2+1 factors as $(x-\alpha)g(x)$ for some nonzero $g(x)$ of degree $< \deg(f(x))$. Then in the quotient $F[x]/(x^2+1)$ we have $\overline{x-\alpha}\cdot\overline{g(x)} = 0$, while $\overline{x-\alpha}$ and $\overline{g(x)}$ are nonzero (why?). This proves the "only if" direction.

Now suppose x^2+1 has no root in F. We shall show that $F[x]/(x^2+1)$ is a field. Indeed, by Question 5, every nonzero element of $F[x]/(x^2+1)$ can be (uniquely) expressed as $\overline{ax+b}$ for some $a, b \in F$ with a or b nonzero. If $a = 0$, then $b \neq 0$ and $\overline{b}$ is certainly a unit (its inverse being $\overline{b^{-1}}$). It remains to show that elements of the form $\overline{ax+b}$ with $a \neq 0$ are units in $F[x]/(x^2+1)$. Since $\overline{ax+b} = \overline{a}\cdot\overline{x+b/a}$ and units are closed under multiplication, it is enough to show that elements of the form $\overline{x+c}$ are units. Now we have

$$\overline{x+c}\cdot\overline{-x+c} = \overline{-x^2+c^2} = \overline{1+c^2}$$

(the last equality being because $\overline{-x^2} = \overline{1}$ in the quotient $F[x]/(x^2+1)$). Since $x^2+1=0$ has no solution in F, it follows that $1+c^2 \in F$ is nonzero and hence is invertible. We have

$$\overline{x+c}\cdot\overline{(1+c^2)^{-1}(x+c)} = \overline{1},$$

showing that $\overline{x+c}$ is indeed a unit.

Remark: The statement we proved here is a special case of the following result, which we shall see soon: $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. Note that for degree 2 and 3 polynomials irreducibility is the same as not having any roots in F (why?).

(b) Straightforward calculations show that $x^2+1=0$ has solutions in $\mathbb{F}_p$ for $p = 2, 5, 13$, so that $\mathbb{F}_p[x]/(x^2+1)$ is not a field for these values of p.

Remark: We shall prove later that $\mathbb{F}_p^\times$ is cyclic (in fact, $F^\times$ is cyclic for any finite field F). Using this you can easily deduce that for odd primes p, the equation $x^2+1=0$ has solutions in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.

(c) One easily checks that $x^2+1=0$ does not have a solution in $\mathbb{F}_p$ for $p = 3, 7$. Thus $\mathbb{F}_p[x]/(x^2+1)$ is a field in these case. By Question 5 it has p^2 elements.

(d) We need to replace x^2+1 with a polynomial $f(x) = x^2+\alpha \in \mathbb{F}_5[x]$ which has no roots in $\mathbb{F}_5$. (Again, they key here is irreducibility, but for polynomials of degree 2 that is equivalent to not having roots.) Then an argument similar to the one in Part (a) would show that $\mathbb{F}_5[x]/(f(x))$ is a field, and in view of Question 5 it has 5^2 elements.

Calculating the squares of elements of $\mathbb{F}_5$ we see that $0, 1, 4$ are squares, while $2, 3$ are not. The polynomial $f(x) = x^2-2$ does the job. (That is, $\mathbb{F}_5[x]/(x^2-2)$ is a field with 25 elements.)