MATH 521A: Abstract Algebra
Homework 10 Solutions

1. Prove that $T = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$. Note that $\mathbb{Q}$ is a subfield of T.

We first note that $0 = 0 + 0\sqrt{2} \in T$. Second, we calculate $(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2} \in T$, so T is closed under subtraction. Lastly, we calculate $(a+b\sqrt{2})(a'+b'\sqrt{2}) = (aa'+2bb')+(ab'+ba')\sqrt{2} \in T$, so T is closed under multiplication. Hence T is a subring of $\mathbb{R}$. Lastly, if $a + b\sqrt{2}$ is nonzero, then neither is $a - b\sqrt{2}$, and so neither is their product $a^2 - 2b^2$. We calculate $(a + b\sqrt{2})(\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}) = \frac{a^2-2b^2}{a^2-2b^2} + \frac{0}{a^2-2b^2}\sqrt{2} = 1$. Hence T is a field.

2. Let F, G be rings such that $\mathbb{Q}$ is a subring of each. Suppose $f : F \to G$ is a (ring) isomorphism. Prove that, for every $a \in \mathbb{Q}$, in fact $f(a) = a$.

First, we recall from Thm 3.10 (or prove from scratch) that $f(0) = 0$ and $f(1) = 1$. Second, for $n \in \mathbb{N}$, we have $f(n) = f(1 + 1 + \cdots + 1) = f(1) + f(1) + \cdots + f(1) = 1 + 1 + \cdots + 1 = n$. Third, for $m, n \in \mathbb{N}$, we have $n = f(n) = f(\frac{n}{m} + \frac{n}{m} + \cdots + \frac{n}{m}) = f(\frac{n}{m}) + f(\frac{n}{m}) + \cdots + f(\frac{n}{m}) = mf(\frac{n}{m})$. Dividing both sides by m, we get $\frac{n}{m} = f(\frac{n}{m})$. Lastly, for $m, n \in \mathbb{N}$, we have $0 = f(0) = f(\frac{n}{m} + \frac{-n}{m}) = f(\frac{n}{m}) + f(\frac{-n}{m}) = \frac{n}{m} + f(\frac{-n}{m})$, so $-\frac{n}{m} = f(\frac{-n}{m})$.

3. Prove that $R = \mathbb{Q}[x]/(x^2 - 2)$ is not isomorphic to $S = \mathbb{Q}[x]/(x^2 - 3)$. Hint: problem 2.

We argue by contradiction; suppose $f : R \to S$ were an isomorphism. Both fields have $\mathbb{Q}$ as subrings, so we may apply problem 2 to conclude that $f([2]_R) = [2]_S$. We now calculate $0_S = 0_R = f([x^2-2]_R) = f([x]_R^2 - [2]_R) = f([x]_R)^2 - f([2]_R) = f([x]_R)^2 - [2]_S$, and hence $f([x]_R)^2 = [2]_S$. Now, $f([x]_R) = [ax + b]_S$, so $[2]_S = [(ax + b)^2]_S = [a^2x^2 + 2abx + b^2]_S = [2abx + (3a^2 + b^2)]_S$. Hence we have some $a, b \in \mathbb{Q}$ satisfying $2ab = 0$ and $3a^2 + b^2 = 2$. The first equation means that $a = 0$ (which leads to $b = \pm\sqrt{2} \notin \mathbb{Q}$), or $b = 0$ (which leads to $a = \pm\sqrt{2/3} \notin \mathbb{Q}$). Hence we have a contradiction.

4. Prove that $R = \mathbb{Q}[x]/(x^2 - 2)$ is isomorphic to $S = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

The natural isomorphism to try is $f : [bx + a]_R \mapsto a + b\sqrt{2}$. There are four things to check. We calculate $f([bx+a]+[b'x+a']) = f([(b+b')x+(a+a')]) = (a+a')+(b+b')\sqrt{2} = (a + b\sqrt{2}) + (a' + b'\sqrt{2}) = f([bx + a]) + f([b'x + a'])$. The slightly tricky one is $f([bx + a][b'x + a']) = f([bb'x^2 + (ba' + ab')x + aa']) = f([(ba' + ab')x + (2bb' + aa')]) = (2bb' + aa') + (ba' + ab')\sqrt{2} = (a + b\sqrt{2})(a' + b'\sqrt{2}) = f([bx + a])f([b'x + a'])$. Suppose that $f([bx + a]) = f([b'x + a'])$. Then $a + b\sqrt{2} = a' + b'\sqrt{2}$, so $a = a', b = b'$ and $[bx + a] = [b'x + a']$. This proves injectivity. Lastly, let $a + b\sqrt{2} \in S$. We have $f([bx + a]) = a + b\sqrt{2}$. This proves surjectivity.

5. Set $F = \mathbb{Z}_3[x]/(x^3 - x + 1)$. Prove that $f(x) = x^3 - x + 1$ splits in F. That is, find three distinct roots of $f(x)$ in F.

The easiest root is $[x]$; we have $f([x]) = [x^3 - x + 1] = [0]$ in F. To find the others takes a bit of trial and error. We have $f([x+1]) = [(x+1)^3-(x+1)+1] = [x^3+3x^2+2x+1] = [x^3 - x + 1] = [0]$ in F. Lastly, we have $f([x-1]) = [(x-1)^3 - (x-1) + 1] = [x^3 - 3x^2 + 2x + 1] = [x^3 - x + 1] = [0]$ in F.

6. Prove that $\{1, \sqrt{2}, i, i\sqrt{2}\}$ is linearly independent over $\mathbb{Q}$.

   Suppose we have $0 = a1+b\sqrt{2}+ci+di\sqrt{2}$, for some $a, b, c, d \in \mathbb{Q}$. First, we consider the real and imaginary parts separately; this tells us that $0 = a1 + b\sqrt{2}$ and $0 = ci + di\sqrt{2}$. Dividing the latter by i, we get $0 = c1 + d\sqrt{2}$. Now, if b is nonzero, we have $\sqrt{2} = \frac{-a}{b}$, a contradiction since $\sqrt{2} \notin \mathbb{Q}$. Hence $b = 0$ and hence $a = 0$. Similarly, $c = d = 0$.

7. Set $R = \mathbb{Q}(\sqrt{2})$, and $S = R(i)$. Determine $[R : \mathbb{Q}]$, $[S : R]$, and $[S : \mathbb{Q}]$.

   The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is x^2-2; this is irreducible by Eisenstein ($p = 2$). Hence $[R : \mathbb{Q}] = 2$. Now, $i \in S$ but $i \notin R$, so $[S : R] \geq 2$. A polynomial whose root is i, over R (and over $\mathbb{Q}$) is $x^2 + 1$. If this were reducible, then $[S : R] < 2$, which we know isn't true, so this is irreducible. Hence $[S : \mathbb{Q}] = [S : R][R : \mathbb{Q}] = 2 \cdot 2 = 4$.

8. Prove that $x^4 - 2x^2 + 9$ is the minimal polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$. (remember to prove irreducibility)

   First, we evaluate $(i + \sqrt{2})^4 - 2(i + \sqrt{2})^2 + 9 = 0$, so $i + \sqrt{2}$ is a root. Since the polynomial has real coefficients, the conjugate, $i - \sqrt{2}$, is also a root. Since the polynomial is even, the negatives of these are also roots. Hence, over $\mathbb{C}$, the polynomial factors as $(x-i-\sqrt{2})(x-i+\sqrt{2})(x+i-\sqrt{2})(x+i+\sqrt{2})$. None of these four linear factors are in $\mathbb{Q}[x]$, but it's possible it has two quadratic factors. If so, the linear factors would break into two pairs. However, $(x - i - \sqrt{2})(x + i + \sqrt{2}) = x^2 - 2i\sqrt{2} - 1 \notin \mathbb{Q}[x]$, and $(x - i - \sqrt{2})(x - i + \sqrt{2}) = x^2 - 2ix - 3 \notin \mathbb{Q}[x]$, and $(x - i - \sqrt{2})(x + i - \sqrt{2}) = x^2 - 2\sqrt{2}x + 3 \notin \mathbb{Q}[x]$. Hence the polynomial is irreducible over $\mathbb{Q}$. Since it is monic, it is the minimal polynomial for all four of these roots.

9. Set $T = \mathbb{Q}(i + \sqrt{2})$, and let R, S be as in problem 7. Prove that $1, \sqrt{2}, i, i\sqrt{2}$ are all in T, so $S \subseteq T$.

   First, $1 \in T$ since $\mathbb{Q} \in T$. Second, $(i + \sqrt{2})^2 = 1 + 2i\sqrt{2} \in T$, so $2i\sqrt{2} \in T$ (since $1 \in T$) and hence $i\sqrt{2} \in T$ (since $2 \in T$). Now, $(i + \sqrt{2})(i\sqrt{2}) = 2i - \sqrt{2} \in T$. Hence $(i + \sqrt{2}) + (2i - \sqrt{2}) = 3i \in T$, and hence $i \in T$ (since $3 \in T$). Lastly, $(i + \sqrt{2}) - i = \sqrt{2} \in T$. Since each basis element of S is in T, all of S is in T.

10. Let R, S, T be as in problems 7 and 9. Determine $[T : \mathbb{Q}]$, and hence $[T : S]$. What can we conclude about S, T?

    We have $[T : \mathbb{Q}] = 4$, since the minimal polynomial is of degree 4. But also $[T : \mathbb{Q}] = [T : S][S : \mathbb{Q}] = [T : S]4$. Hence $[T : S] = 1$, and in fact $S = T$.