Solutions to Assignment 9

1. Show that the only irreducible elements in the ring of integers are of the form $\pm p$ where p is a prime number.

> **Solution:** If an integer n is irreducible, then it cannot be written in the form $n = a \cdot b$ unles one of a or b is a unit. The only units in the ring of integers are ± 1. So, if we assume than n is positive, then this is the same as the condition that n is prime.

2. Show that the elements of the form $T - a$ in the ring $\mathbb{Q}[T]$ are irreducible. (This is true with any field.)

> **Solution:** If we write $T - a = P(T)Q(T)$, then sum of the degrees of P and Q is 1. This means that one of the degrees is 0. In that case, it is a constant and ths a unit.

3. If p is an irreducible element of R and p lies in the ideal $q \cdot R$, then show that either q is a unit (so that $q \cdot R = R$) or $q = p \cdot u$ where u is a unit.

> **Solution:** We have $p = q \cdot a$. By the definition of irreducibility, either q or a is a unit. If q is not a unit then a is a unit and $q = p \cdot u$ where u is such that $a \cdot u = 1$.

4. Check that P is a prime ideal if and only if R/P is a domain.

> **Solution:** If R/P is a domain, then it has no non-zero zero divisors. In other words, if a and b are in R so that $a \cdot b$ is 0 in R/P, then either a is 0 in R/P or b is 0 in R/P. This is the same as saying that either a is in P or b is in P. The converse condition is similar.

5. Check that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Show that 2 does not divide $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$ in the ring R.

> **Solution:** The ring R is contained in the field of complex numbers. So every element can be *uniquely* expressed in the form $a + b\sqrt{-5}$ with a and b in the field of real numbers. In particular, $1/2 \pm (1/2)\sqrt{-5}$ is not in the ring R.

6. Check that $1 + \sqrt{-5} = \alpha \cdot \beta$ with α and β in R is only possible if either α or β is ± 1.

Solution: We write $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Calculating the modulus of the complex numbers we have

$$1 + 5 = 6 = (a^2 + 5b^2)(c^2 + 5d^2)$$

Now the expression $p^2 + 5q^2$ takes the values 0,1,6,... when p and q are integers. This, the only way for the above equation to be true is that either $a^2 + 5b^2$ or $c^2 + 5d^2$ is 1. This proves that either α or β is ± 1.

7. Conclude that $1 + \sqrt{-5}$ is irreducible but not prime.

Solution: From the above exercise we see that $1 + \sqrt{-5}$ is irreducible. However, as seen in the exercise before that we have $2 \cdot 3 = 6$ lies in $(1 + \sqrt{-5}) \cdot R$, but neither 2 nor 3 lies in this ideal.

8. Show that if P is a maximal ideal then R/P is a field.

Solution: If a is not in P, then $a \cdot R + P = R$ by the maximality of P. This means that we have an equation of the form $a \cdot b + p = 1$ where p lies in the ideal P. Thus $a \cdot b = 1$ in R/P and so a is a unit in R/P.

9. Conversely, if I is an ideal in a commutative ring R and R/I is a field, then show that I is a maximal ideal.

Solution: Since R/I is a field $1 \neq 0$ in it, so 1 does not lie in I and so I is a proper ideal.

If a is any element of R which is not in I, then there is an element b in R so that $a \cdot b = 1$ in R/I. This means that $a \cdot b - 1 = c$ lies in I. Hence 1 lies in $a \cdot R + I$ and so $a \cdot R + I = R$ (since it is closed under multiplication by R). This shows that I is a maximal ideal.

10. If u is a unit in a ring R and $u = a \cdot b$, then show that a and b are units in R.

Solution: Let v be in R so that $u \cdot v = 1 = v \cdot u$. We then have $a \cdot (b \cdot v) = 1$ and $(v \cdot a) \cdot b = 1$. This shows that a and b are units.

11. If a prime q is a multiple of a prime p in a domain R then show that $q = p \cdot u$ where u is a unit. (Hint: Look at the proof that primes are irreducible.)

Solution: If q lies in the ideal $p \cdot R$, then $q = p \cdot u$ for some u in R. This means that $p \cdot u$ lies in $q \cdot R$ which is a prime ideal. Hence, either p lies in $q \cdot R$ or u lies in $q \cdot R$. In the first case $p = q \cdot v$ so $p = p \cdot u \cdot v$. Since a prime is non-zero, we can cancel p to get that u is a unit. If u lies in $q \cdot R$, then $u = q \cdot b$ so $u = p \cdot b \cdot u$. Since q is a prime it is non-zero; this means u is non-zero since q is a multiple of u. Hence we can cancel it to get $p \cdot b = 1$. This contradicts the fact the p is a prime and hence a non-unit.

12. If a is an element of a PID R which is not a multiple of a prime p, then show that $a \cdot R + p \cdot R = R$. (Hint: a gives a non-zero element of R/p which is a field.)

Solution: If the ideal $a \cdot R + p \cdot R$ is a proper ideal in R, then it is contained in a maximal ideal I of R. Since R is a PID, $I = q \cdot R$ for some q. Since maximal ideals are prime, q is a prime. Thus the prime p is a multiple of the prime q and it follows that q is a multiple of q by the previous exercise. It follows that a is a multiple of p contradicting the hypothesis that a is *not* a multiple of p. Hence it follows that $a \cdot R + p \cdot R = R$.

13. Find polynomials $A(T)$ and $B(T)$ so that $A(T) \cdot T + B(T) \cdot (T^2 - 1) = 1$.

Solution: We can take $A(T) = T$ and $B(T) = -1$. We then have

$$T \cdot T - 1 \cdot (T^2 - 1) = 1$$

14. Use the above to find a polynomial $C(T)$ which is divisible by T so that its reduction modulo $T^2 - 1$ is equivalent to $T + 1$.

Solution: Multiplying the above equation by $T + 1$, we have

$$T \cdot T \cdot (T + 1) - (T^2 - 1) \cdot (T + 1) = (T + 1)$$

Thus, we have $C(T) = T^3 + T^2$

15. Find an integer n so that it is 7 modulo 8 and 8 modulo 9.

Solution: We have the equation $9 - 8 = 1$. Thus, $7 \cdot 9 = 63$ is 7 modulo 8 and 0 modulo 9. Now 8 is 8 modulo 9 and 0 modulo 8. So $63 + 8 = 71$ is the solution to the problem.

16. Given a and b distinct rational numbers, find a matrix S (in terms of a and b) so that

$$S^{-1} \cdot \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \cdot S = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Solution: We need to find column vectors v and w so that

$$\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \cdot v = a \cdot v$$

and

$$\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \cdot w = b \cdot w$$

Equivalently, we want

$$\begin{pmatrix} 0 & 1 \\ 0 & b-a \end{pmatrix} \cdot v = 0$$

and

$$\begin{pmatrix} a-b & 1 \\ 0 & 0 \end{pmatrix} \cdot w = 0$$

We check easily that

$$v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } w = \begin{pmatrix} 1 \\ b-a \end{pmatrix}$$

Satisfy these equations. Hence

$$S = \begin{pmatrix} 1 & 1 \\ 0 & b-a \end{pmatrix}$$

gives a solution to the problem

17. Given a and $b \neq 0$ rational numbers, find a matrix S (in terms of a and b) so that

$$S \cdot \begin{pmatrix} a-b & b \\ -b & a+b \end{pmatrix} \cdot S^{-1} = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$$

Solution: As above we need to find column vectors v and w so that

$$\begin{pmatrix} a-b & b \\ -b & a+b \end{pmatrix} \cdot v = a \cdot v$$

and

$$\begin{pmatrix} a-b & b \\ -b & a+b \end{pmatrix} \cdot w = v + a \cdot w$$

We re-write the first equation as

$$\begin{pmatrix} -b & b \\ -b & b \end{pmatrix} \cdot v = 0$$

which has the solution $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. We can then re-write the second equation as

$$\begin{pmatrix} -b & b \\ -b & b \end{pmatrix} \cdot w \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

This has the solution

$$w = \begin{pmatrix} -\frac{1}{2b} \\ \frac{1}{2b} \end{pmatrix}$$

Thus, the required matrix is

$$S = \begin{pmatrix} 1 & -\frac{1}{2b} \\ 1 & \frac{1}{2b} \end{pmatrix} \cdot v = 0$$

18. Show that $T^2 + 1$ is irreducible in $\mathbb{Q}[T]$

Solution: If $T^2 + 1$ has a factorisation, then at least one factor is linear. it follows that we must have a rational number so that its square is -1. However, the square of any rational number is positive. Hence, this is not possible.

19. Show that $T^3 - T + 1$ is irreducible.

Solution: If $P(T) = T^3 - T + 1$ has a factorisation, then at least one factor is linear. If p/q is a root then we have $p^3 - pq^2 + q^3 = 0$. So any prime that divides q also divides p. It follows that $p/q = n$ is an integers. Now $P'(T) = 3T^2 - 1$ is positive for $T \geq 1$ and $P(1) = 1 > 0$. It follows that $P(T)$ is positive for $T \geq 1$. Similarly, $P'(T)$

is positive for $T \leq -1$ and $P(-1) = -1 < 0$. Thus $P(T)$ is negative for $T \leq -1$. Thus, its only integer can be at 0. However $P(0) = 1$ is non-zero. Thus $P(T)$ has no integer 0 and so it is irreducible.

20. Check that the Liebnitz rule is satisfied by the formal derivative.

$$(P(T) \cdot Q(T))' = P'(T)Q(T) + P(T)Q'(T)$$

Solution: We only need to check this for $P(T) = T^a$ and $Q(T) = T^b$ in which case it is trivial.

21. Check that the following identity holds:

$$P'(T) = \sum_{i=1}^{n} \frac{(T - z_1) \cdots (T - z_n)}{(T - z_i)}$$

Solution: This follows from the Liebniz rule.

22. (Starred) Show that the converse is also true. If $P(T)$ and $P'(T)$ have a common factor, then there is a repeated root.

Solution:

23. Find an integer n so that $n^2 + 1$ is divisible by 125 ($= 5^3$).

Solution: We have $2^2 + 1 = 5$ is divisible by 5. So we look for $a = 2 + 5k$ so that $a^2 + 1$ is divisible by 25. We see that $7 = 2 + 5$ satisfies this property. Next we look for $b = 7 + 25k$ so that $b^2 + 1$ is divisible by 125. We note that

$$(7 + 25k)^2 + 1 = 49 + 1 + 2 \cdot 7 \cdot 25k \pmod{125} = 25(2 + 14k)$$

We need $2 + 14k$ to be divible by 5 and that works for $k = 2$. Thus we see that $n = 57$ solves the problem.

24. Find a polynomial $P(T)$ so that $P(T)^3 - 1$ is divisible by $(T^3 - 1)^2$.

Solution: We note that $P_0(T)$ has the property that $P_0(T)^3 - 1$ is divisible by $(T^3 - 1)$. So we look for $P(T) = T + A(T)(T^3 - 1)$. We get

$$P(T)^3 - 1 = T^3 - 1 + 3 \cdot T^2 \cdot A(T)(T^3 - 1) \pmod{(T^3-1)^2} = (T^3 - 1)(1 + 3T^2 A(T))$$

So we need to find $A(T)$ so that $1 + 3T^2 A(T)$ is divisible by $T^3 - 1$. Clearly $A(T) = -(1/3)T$ works. Thus we have $P(T) = T - (1/3)T(T^3 - 1)$.