Primes, Irreducibles, Maximal Ideals, Factorisation, Block Form (contd.)

1. Show that the only irreducible elements in the ring of integers are of the form $\pm p$ where p is a prime number.
2. Show that the elements of the form $T - a$ in the ring $\mathbb{Q}[T]$ are irreducible. (This is true with any field.)
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.
4. Check that P is a prime ideal if and only if R/P is a domain.
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.
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.
7. Conclude that $1+\sqrt{-5}$ is irreducible but not prime.
8. Use the above reasoning to conclude that, if P is a maximal ideal then R/P is a field.
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.
10. Given a maximal ideal P, try to prove directly that if $a \cdot b$ lies in P and a does not lie in P then b lies in P.
11. If u is a unit in a ring R and $u = a \cdot b$, then show that a and b are units in R.
12. 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.)
13. 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.)
14. Find polynomials $A(T)$ and $B(T)$ so that $A(T) \cdot T + B(T) \cdot (T^2 - 1) = 1$.
15. 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 $T + 1$.
16. Find an integer n so that it is 7 modulo 8 and 8 modulo 9.
17. Given a and b distinct rational numbers, find a matrix S (in terms of a and b) so that

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

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

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

19. Show that $T^2 + 1$ is irreducible.

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

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

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

22. Check that the following identity holds:

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

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

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

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