Solution Set to HW 6:

1a.] We must check it's a subgp:

(i) Closure under operations:

If $f, g \in R$

Then $\frac{d}{dt}(fg)|_{t=0} = f(0)g'(0) + f'(0)g(0) = 0$.

$\frac{d}{dt}(f+g)|_{t=0} = f'(0) + g'(0) = 0$

Thus, fg and $f+g \in R$.

Closure under inverses:

If $f \in R$,

$\frac{d}{dt}(-f)|_{t=0} = -\frac{d}{dt}(f)|_{t=0} = 0$.

Hence $-f \in R$.

(ii) Identity elements:

$\frac{d}{dt}|_{t=0}(1) = \frac{d}{dt}|_{t=0}(0) = 0$.

[b.] Given any polynomial $a_0 + a_1 t + \cdots + a_n t^n = f$

$f \in R \iff \frac{d}{dt}(f) = 0 \iff a_1 = 0$

Thus, it is the set of all polynomials with no constant term.

$k[T^2, T^3]$ = all linear combinations of polynomials of the form T^{2m+3n} $m \geq 0, n \geq 0$. It is easy to check that $2m+3n$ will be equal to all numbers except 1. Hence this is also the polynomial ring without constant terms. Thus $R = k[T^2, T^3]$

Now define a map

$$\varphi : k[X, Y] \to k[T^2, T^3]$$

$$X \to T^3$$
$$Y \to T^2$$

This map is clearly surjective. It is also clear that the only imposed relationship on the factors is $(T^3)^2 = (T^2)^3 = T^6$. (A more rigorous proof can be formed by using the multivariable factor theorem.) Thus $\ker \varphi = (X^2 - Y^3)$.

(1-7)

(c) Suppose this were not true then since R is a domain one of the factors dividing it would have to be monic which we already established is not the case in part (b). Thus $(T^2)^3 = (T^3)^2$ is two factorizations into irreducibles.

2a] If $f \not\equiv 0 \pmod p$ then the image in $\mathbb{F}_p[X]$ is non-zero. (given by quotienting out by a prime p.) Since f is non-zero and $\mathbb{F}_p[X]$ is a domain we have the cancellation law. Thus $fg = fh \pmod p \iff g = h \pmod p$.

b]
$$(X-1)^p = X^p - \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-2} + \dots + (-1)^p$$

It is easy to see that $\binom{p}{k} = \frac{p!}{(p-k)!\,k!}$

Will be divisible by p for $1 \le k \le p$ since the numbers making up the denominator will all be less than p and therefore cannot divide since a prime by definition is only divisible by $\pm 1, \pm p$. Thus.

$$(X-1)^p \equiv X^p + (-1)^p$$

If $p = 2$: $X^p + 1 \equiv X^p - 1$.

If p is odd: $X^p + (-1) \equiv X^p - 1$

Now the second part follows from dividing both sides by $X-1$. This will hold in any field in particular, $\mathbb{F}_p[X]$.

(c) $c(X) \nmid X-1$ since $\mathbb{F}_p$ is a field and thus a domain so we may use a degree argument. (Except when $p=2$) (So this will not work there!)

Now we have the commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{c(X)} & \mathbb{Z}[X]/c(X) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle (p)} \\ \mathbb{F}_p[X] & \xrightarrow{c(X)} & \mathbb{F}_p[X]/c(X) \end{array}$$

All the maps are quotient maps and therefore surjective. Showing an ideal is prime is equivalent to showing that the image of the quotient map is the domain. Thus, it suffices to show

$\mathbb{F}_p[X]/c(X)$ is not a domain

Well $c(X) \nmid (X-1) \Rightarrow (X-1)$'s image is not 0 in the above ring well $(X-1)^p = c(X) = 0 \to$ in the above ring. Here, the image of $\overline{X-1}$ is a zero divisor, meaning $\mathbb{F}_p[X]/c(X)$ is not a domain.

3.] For the first use eisenstein's criteron. when $p=3$. For the second take it mod 2. It is irreducible here so it must be irreducible. by preservation of degree.

4.] Take $u+v=r$.
$u \cdot v = s$.

Consider the polynomial.

$$X^2 - rx + s = (x-u)(x+u).$$

Finding u, v satisfying the above equation in complex numbers is equivalent to finding roots of the above polynomial in $\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed. we are done.

(The rest is a long computation. that may be found online.)