Math 121. Quotient of a PID

In class we used linear algebra to prove that if $f \in k[X]$ is irreducible then $k[X]/(f)$ is a field. In this handout, we give a proof without linear algebra by showing a more general result for the quotient ring of *any* PID modulo an irreducible element.

Let R be a PID (so it is a UFD), and choose $r \in R$ that is irreducible. The quotient ring $R/(r)$ is a domain. Indeed, this amounts to the assertion that if $a, b \in R$ and $r|ab$ then $r|a$ or $r|b$, a property which follows from the irreducibility of r and the fact that R is a UFD. But we claim more: $R/(r)$ is a *field*.

Example 0.1. Before proving this property of $R/(r)$, we note a basic example: $R = \mathbf{Z}[i]$ (a Euclidean domain, hence a PID) and $r = 3$. The element 3 is irreducible in $\mathbf{Z}[i]$ (you will prove this in HW5), and $3\mathbf{Z}[i] = \{3a + 3bi \mid a, b \in \mathbf{Z}\}$ so one can see (check!) that $\mathbf{Z}[i]/3\mathbf{Z}[i]$ has size 9. So this is a finite field of size 9 (not to be confused with $\mathbf{Z}/9\mathbf{Z}$, which isn't even a domain).

Let's now prove that $R/(r)$ is a field! Pick a nonzero element in $R/(r)$, so it has a representative $a \in R$ not divisible by r. We seek a multiplicative inverse in $R/(r)$, which is to say we seek $x \in R$ such that $ax \equiv 1 \bmod r$. Equivalently, we seek $x, y \in R$ such that $ax - 1 = ry$, or in other words $ax + r(-y) = 1$. Put another way, we aim to show that if $a \in R$ does not lie in (r) then the ideal (a, r) of R contains 1, which is to say that it is R itself (as an ideal).

Since R is a PID, the ideal (a, r) has a generator, say d. This is an element of the form $d = ax + ry$ such that $a, r \in (d)$. In particular, $d|r$. But r is irreducible, so at the cost of replacing d with an $R^\times$-multiple (as we may do without affecting that it generates (a, r)) we can arrange that either $d = 1$ or $d = r$. But $d|a$ and by design $a \notin (r)$, so $d \neq r$. Hence, $d = 1$. But $d = ax + ry$ for some $x, y \in R$, so $ax \equiv 1 \bmod r$. This gives the multiplicative inverse that we sought.