Worksheet 18

Math 391, Abstract Algebra

Friday, November 13, 2020

Consider Euclid's lemma for integers and polynomials:

Chapter 1, Proposition 2.5: Let $p, a, b \in \mathbb{Z}$. If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Chapter 3, Proposition 1.7: Let F be a field and $f, g, h \in F[x]$. If f is irreducible and $f \mid gh$, then $f \mid g$ or $f \mid h$.

Here is a proof for integers:

Because p is prime, we either have $\gcd(p, b) = p$ or $\gcd(p, b) = 1$. In the first case, p divides b. In the second case, we can write

$$1 = pm + bn$$

for some $m, n \in \mathbb{Z}$. Multiply through by a to get

$$a = apm + abn.$$

Because $p \mid ab$, we can write $ab = pc$ for some $c \in \mathbb{Z}$. Thus

$$a = apm + pcn = p(am + cn),$$

so $p \mid a$.

Convince yourselves that the same proof works for polynomials. Are there any statements that need more explanation in this case?

Challenge: With integers, we saw that the conclusion of Euclid's lemma fails if p is not prime: for example, 6 is not prime, and we have $6 \mid 3 \cdot 4$ but $6 \nmid 3$ and $6 \nmid 4$. Find similar counterexamples with polynomials when f is reducible.