Math 430 – Problem Set 7 Solutions

Due April 22, 2016

18.10. (a) Prove that every field contains a unique prime subfield.

Solution. Suppose that F is a field, and let E be the intersection of all subfields of F. We show that E is the unique prime subfield of F.

Note that $0, 1 \in E$, so E is nonempty. If $a, b \in E$ then $a, b \in L$ for every subfield L of F, so $a + b$, $a - b$, ab and a/b are in L, and thus all in E. Thus E is a subfield.

If $L \subset E$ is a proper subfield, then L is a subfield of F as well. This contradicts the definition of E, since E is contained in every subfield of F. Thus E is a prime field.

Finally, supposed E' is another prime subfield of F. By the construction of E, $E \subseteq E'$. Since E' is a prime subfield, we must have $E' = E$.

(b) If F is a field of characteristic 0, prove that the prime subfield of F is isomorphic to $\mathbb{Q}$.

Solution. Define a homomorphism $\phi : \mathbb{Z} \to F$ by $\phi(n) = n \cdot 1_F$. Since F has characteristic 0, this homomorphism is injective, so its image is a subring of F isomorphic to $\mathbb{Z}$. Now by Theorem 18.4, F contains a subfield isomorphic to $\mathbb{Q}$. Since $\mathbb{Q}$ has no subfields it is prime, and thus by part (a) is the unique prime subfield of F.

(c) If F is a field of characteristic p, prove that the prime subfield of F is isomorphic to $\mathbb{Z}_p$.

Solution. Define $\phi : \mathbb{Z} \to F$ as in part (b). Since F has characteristic p, ϕ has kernel $p\mathbb{Z}$ and thus by the first isomorphism theorem its image is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, which is a prime field. By part (a), this is the unique prime subfield of F.

18.11. (d) Prove that $\mathbb{Z}[\sqrt{2}i]$ is a Euclidean domain under the Euclidean valuation $\nu(a + b\sqrt{2}i) = a^2 + 2b^2$.

Solution. I first claim that $\nu(xy) = \nu(x)\nu(y)$ for $x, y \in \mathbb{Q}[\sqrt{2}i]$, since

$$\begin{aligned}
\nu((a + b\sqrt{2}i)(c + d\sqrt{2}i)) &= \nu((ac - 2bd) + (ad + bc)\sqrt{2}i) \\
&= (ac - 2bd)^2 + 2(ad + bc)^2 \\
&= a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2 \\
\nu(a + b\sqrt{2}i)\nu(c + d\sqrt{2}i) &= (a^2 + 2b^2)(c^2 + 2d^2) \\
&= a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2.
\end{aligned}$$

For nonzero $a+b\sqrt{2}i \in \mathbb{Z}[\sqrt{2}i]$ we have $\nu(a+b\sqrt{2}i) = a^2+2b^2 \geq 1$. Thus $\nu(x) \leq \nu(xy)$ for $x, y \in \mathbb{Z}[\sqrt{2}i]$ with $y \neq 0$.

Now suppose $a + b\sqrt{2}i, c + d\sqrt{2}i \in \mathbb{Z}[\sqrt{2}i]$ with $c + d\sqrt{2}i$ nonzero. Let q_1 be the closest integer to $\frac{ac+2bd}{c^2+2d^2}$ and q_2 the closest integer to $\frac{bc-ad}{c^2+2d^2}$. Define s_1, s_2, r_1, r_2 by

$$\begin{aligned}
s_1 + s_2\sqrt{2}i &= \left(\frac{ac + 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{2}i\right) - (q_1 + q_2\sqrt{2}i), \\
r_1 + r_2\sqrt{2}i &= (a + b\sqrt{2}i) - (q_1 + q_2\sqrt{2}i)(c + d\sqrt{2}i).
\end{aligned}$$

We need to show that $r_1^2 + 2r_2^2 < c^2 + 2d^2$. Note that $|s_1| \leq 1/2$ and $|s_2| \leq 1/2$ by the definition of q_1 and q_2. Moreover,

$$(s_1 + s_2\sqrt{2}i)(c + d\sqrt{2}i) = (a + b\sqrt{2}i) - (q_1 + q_2\sqrt{2}i)(c + d\sqrt{2}i) = r_1 + r_2\sqrt{2}i.$$

Thus

$$\nu(r_1 + r_2\sqrt{2}i) = \nu(s_1 + s_2\sqrt{2}i)\nu(c + d\sqrt{2}i) \leq (\frac{1}{4} + 2 \cdot \frac{1}{4})\nu(c + d\sqrt{2}i) < \nu(c + d\sqrt{2}i)$$

as desired.

18.14. Let D be a Euclidean domain with Euclidean valuation ν. If u is a unit in D, show that $\nu(u) = \nu(1)$.

Solution. Since u is a unit we can find $v \in D$ with $uv = 1$. Then $\nu(u) \leq \nu(uv) = \nu(1) \leq \nu(1 \cdot u) = \nu(u)$. So all of the inequalities must be equalities and we have $\nu(u) = \nu(1)$.

18.17. Prove or disprove: Every subdomain of a UFD is also a UFD.

Solution. We showed in class that $\mathbb{Z} + x\mathbb{Q}[x]$ was not a UFD. But $\mathbb{Z} + x\mathbb{Q}[x]$ is a subdomain of $\mathbb{Q}[x]$, which is a UFD.