Math 418, Spring 2024 – Practice Problems 1

8.1.10 *Prove that the quotient ring* $\mathbb{Z}[i]/I$ *is finite for any nonzero ideal* I *of* $\mathbb{Z}[i]$.

Solution. $\mathbb{Z}[i]$ is Euclidean, hence a PID, so $I = (\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. If $\beta \in \mathbb{Z}[i]$, The Euclidean algorithm guarantees that $\beta = q\alpha + r$ for some $q, r \in \mathbb{Z}[i]$ where $N(r) < N(\alpha)$. But since $N(z) = |z|^2$ and $\mathbb{Z}[i]$ is discrete, there are only finitely many such points; hence finitely many cosets.

8.1.11 (See D & F for problem)

(a) Let m be an lcm of a and b. Then $m \in (a) \cap (b)$. Suppose $(n) \subseteq (a) \cap (b)$; then n is a common multiple of a and b, so by uniqueness of lcm, $m|n$. If also $n|m$, then $(m) = (n)$, and if it doesn't, $(n) \subsetneq (m)$.

(b) Uniqueness follows from part a. For existence, since Euclidean domains are PIDs, the ideal $(a) \cap (b)$ (intersection of ideals is an ideal) is principal, say equaling (m). That m is an lcm of a and b can now be proved directly from the definition.

(c) Let d be a gcd of a and b and let $m := ab/d$. m is a multiple of a since $m = a \cdot \frac{b}{d}$, and similar for b. Conversely, if n is a least common multiple of a and b, then $m = nk$, so $n = \frac{m}{k} = a \cdot \frac{b}{dk}$ is a multiple of a and thus b is a multiple of dk. Similarly, a is a multiple of dk, so k is a unit.

8.2.4 Let I be nonprincipal, and let $a_1 \in I, b_1 \in I \setminus (a_1)$. Let a_2 be a gcd of a_1 that (by condition (i)) is in I. Since $b_1 \notin I$, it can't be an associate of a_1, so $(a_1) \subsetneq (a_2)$. Let $b_2 \in I \setminus (a_2)$. Continue, getting a sequence $a_1, a_2, \ldots$ with $a_{i+1}|a_i$ where no a_{i+1} is an associate of a_i, contradicting condition (ii).

8.3.8 (a) This is Homework 1, problem 6

(b) Prove that each ideal is maximal (see hint in D & F)

(c) Both factorizations expand to $I_2^2 I_3 I_3'$ (see Homework 2, Problem 5c)

9.3.4 (see lecture notes)

9.4.1b *Determine whether* $x^3 + x + 1$ *is irreducible in* $\mathbb{F}_3[x]$

Solution. Plug in all field elements to test for roots.

9.4.13 *Prove that* $x^3 + nx + 2$ *is irreducible over* $\mathbb{Z}$ *for all integers* $n \neq 1, -3, -5$.

Solution. Use the rational root theorem.

13.1.2 *Show that* $p(x) = x^3 - 2x - 2$ *is irreducible over* $\mathbb{Q}$ *and let* θ *be a root. Compute* $(1+\theta)(1+\theta+\theta^2)$ *and* $\frac{1+\theta}{1+\theta+\theta^2}$ *in* $\mathbb{Q}(\theta)$.

Solution. Use the rational root theorem to show that $p(x)$ doesn't have a root in $\mathbb{Q}$, and is therefore irreducible. Alternatively, use Eisenstein's criterion with the prime 2.

Since θ is a root of p, $\theta^3 = 2\theta + 2$, so

$$(1+\theta)(1+\theta+\theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 3 + 4\theta + 2\theta^2.$$

For the final part, let $a + b\theta + c\theta^2 = \frac{1+\theta}{1+\theta+\theta^2}$. Then,

$$\begin{aligned} 1+\theta &= (a + b\theta + c\theta^2)(1+\theta+\theta^2) \\ &= a + (a+b)\theta + (a+b+c)\theta^2 + (b+c)\theta^3 + c\theta^4 \\ &= a + (a+b)\theta + (a+b+c)\theta^2 + (b+c)(2\theta+2) + c(2\theta^2+2\theta) \\ &= a + 2b + 2c + (a+3b+4c)\theta + (a+b+3c)\theta^2. \end{aligned}$$

Solving this system of equations gives

$$\frac{1+\theta}{1+\theta+\theta^2} = \frac{1}{3}(1 + 2\theta - \theta^2).$$

13.1.6 *Show that if* α *is a root of* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *then* $a_n\alpha$ *is a root of the monic polynomial* $q(x) = x^n + a_{n-1}x^{n-1} + a_n a_{n-2} x^{n-2} + \cdots + a_n^{n-2} a_1 x + a_n^{n-1} a_0$.

Solution. This follows from the fact that $q(a_n x) = a_n^{n-1} p(x)$.

13.2.2 (This is just a long computation without any tricks; you'll know you got the right answer if you got fields of the right sizes, and the multiplicative groups were cyclic)

13.2.12 *Suppose the degree of the extension* K/F *is a prime* p. *Show that any subfield* E *of* K *containing* F *is either* K *or* F.

Solution. This is a straightforward consequence of the tower law. First note that a degree one field extension is trivial, since the extension field is a dimension-one vector space over the base field, and thus the same field. Then we have $p = [K : F] = [K : E][E : F]$, and since these are all integers one of $[K : E]$ and $[E : F]$ must be p, and the other must be 1.