Midterm 2

Modern Algebra (Math 403)
Instructor: Jarod Alper
Winter 2018
February 23, 2018

Name: $\underbrace{\hspace{6cm}}$

Read all of the following information before starting the exam:

- You may not consult any outside sources (calculator, phone, computer, textbook, notes, other students, ...) to assist in answering the exam problems. All of the work will be your own!
- Write clearly!! You need to write your solutions carefully and clearly in order to convince me that your solution is correct. Partial credit will be awarded.
- Good luck!

Problem	Points
1 (25 points)	______
2 (25 points)	______
3 (25 points)	______
4 (25 points)	______
Total (100 points)	

Problem 1. *As always, make sure your answers are fully justified.*

(a) If p is a prime integer, is the polynomial $f(x) = x^p - p \in \mathbb{Q}[x]$ irreducible?

Solution: Since p is a prime such that (1) p does not divide the leading coefficient of f, (2) p divides all coefficients of f other than the leading coefficient and (3) p^2 does not divide the constant term, we may apply Eisenstein's criterion to conclude that $f(x)$ is irreducible.

(b) Is the polynomial $f(x) = x^4 + 3x + 1 \in \mathbb{Q}[x]$ irreducible?

Solution: By Gauss's lemma, if $f(x) \in \mathbb{Q}[x]$ is reducible, then $f(x)$ has a factorization over $\mathbb{Z}[x]$ as a product of non-constant polynomials in $\mathbb{Z}[x]$. This in turn implies that for every prime integer $p \in \mathbb{Z}$, the image of $f(x)$ under the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p[x]$ is also reducible (Homework Problem 5.6). If we take $p = 2$, then the image of f in $\mathbb{Z}/2[x]$ is $\overline{f}(x) = x^4 + x + 1$. Since $\overline{f}(0) = \overline{f}(1) = 1$, $\overline{f}$ has no linear factors. On the other hand, the only irreducible polynomial in $\mathbb{Z}/2[x]$ of degree 2 is $x^2 + x + 1$ and this polynomial does not divide $\overline{f}$ (indeed, using the division algorithm, we compute that $\overline{f}(x) = (x^2 + x + 1)(x^2 + x) + 1$). Since $\overline{f} \in \mathbb{Z}[x]$ has no linear or quadratic factors, $\overline{f} \in \mathbb{Z}/2[x]$ is irreducible and we may conclude that $f \in \mathbb{Q}[x]$ is irreducible.

Problem 2.

(a) Show that there exists an irreducible polynomial $f \in \mathbb{Z}/2[x]$ of degree 4.

Solution: In Problem 1(b), we saw that $f(x) = x^4 + x + 1 \in \mathbb{Z}/2[x]$ is irreducible.

(b) Show that there exists a finite field with 16 elements.

Solution: Since $\mathbb{Z}/2[x]$ is a PID and $f(x) = x^4 + x + 1 \in \mathbb{Z}/2[x]$ is irreducible, we know from lecture that the ideal $(f) \subset \mathbb{Z}/2[x]$ is maximal. Therefore $\mathbb{Z}/2[x]/(f)$ is a field with 16 elements.

Problem 3.

(a) Let p be a prime integer. Find a factorization of $x^p - x \in \mathbb{Z}/p[x]$ as a product of irreducible polynomials.

Solution: Let $f(x) = x^p - x \in \mathbb{Z}/p[x]$. Fermat's Little Theorem states that $a^p \equiv a \mod p$ for any integer a. In other words, for every element $\alpha \in \mathbb{Z}/p$, $f(\alpha) = 0$ or equivalently $x - \alpha$ divides f. The elements $x - \alpha \in \mathbb{Z}/p[x]$ are pairwise relatively prime and therefore the product $\prod_{\alpha \in \mathbb{Z}/p}(x - \alpha)$ also divides $x^p - x$, but since this product has the same degree and same leading term as the polynomial f, we conclude that

$$f(x) = \prod_{\alpha \in \mathbb{Z}/p} (x - \alpha)$$

and this is the desired factorization since each polynomial $x - \alpha$ is irreducible for $\alpha \in \mathbb{Z}/p$.

(b) Find a factorization of $5 \in \mathbb{Z}[i]$ as a product of irreducible elements.

Solution: Clearly, we have that $5 = (2 + i)(2 - i)$. It remains to show that both $2 + i$ and $2 - i$ are irreducible elements in $\mathbb{Z}[i]$. For a complex number $z = a + bi$, the square of the modulus of z is $|z|^2 = a^2 + b^2$. Suppose $2 + i = xy$ with $x, y \in \mathbb{Z}[i]$. Then $5 = |2 + i|^2 = |x|^2|y|^2$. Since 5 is prime, either $|x|$ or $|y|$ must be 1. It follows that either x or y is a unit. Thus, $2 + i$ is irreducible. The identical argument shows that $2 - i$ is irreducible since $|2 - i|^2$ is also 5.

Problem 4. Show that $\mathbb{Z}[\sqrt{-2}]$ is a UFD.

Solution: It suffices to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain since we may use the theorem in lecture that any Euclidean domain is a UFD. First, clearly $\mathbb{Z}[\sqrt{-2}]$ is an integral domain as it is a subring of the complex numbers. Consider the function

$$N\colon \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}_{\geq 0}, \qquad a + b\sqrt{-2} \mapsto a^2 + 2b^2.$$

Clearly, $N(0) = 0$. We need to show that for any elements $x, y \in \mathbb{Z}[\sqrt{-2}]$ with $y \neq 0$, then there exists $q, r \in \mathbb{Z}[\sqrt{-2}]$ such that $x = qy + r$ and with $N(r) < N(q)$.

Write $x = a + b\sqrt{-2}$ and $y = c + d\sqrt{-2}$. As elements in $\mathbb{C}$, we can write

$$\frac{x}{y} = \frac{a + b\sqrt{-2}}{c + d\sqrt{-2}} = \frac{a + b\sqrt{-2}}{c + d\sqrt{-2}} \cdot \left(\frac{c - d\sqrt{-2}}{c - d\sqrt{-2}}\right) = \left(\frac{ac + bd}{N(y)}\right) + \left(\frac{bc - ad}{N(y)}\right)\sqrt{-2}$$

Choose integers e, f such that $|\frac{ac+bd}{N(y)} - e| \leq \frac{1}{2}$ and $|\frac{bc-ad}{N(y)} - f| \leq \frac{1}{2}$. Then

$$\begin{aligned}
\left|\frac{x}{y} - (e + f\sqrt{-2})\right|^2 &= \left|\left(\frac{ac + bd}{N(y)} - e\right) + \left(\frac{bc - ad}{N(y)} - f\right)\sqrt{-2}\right|^2 \\
&= \left(\frac{ac + bd}{N(y)} - e\right)^2 + 2\left(\frac{bc - ad}{N(y)} - f\right)^2 \\
&\leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4} \\
&< 1
\end{aligned}$$

Let $q = e + f\sqrt{-2}$ and $r = x - qy$. Then clearly we have that $x = qy + r$. Moreover,

$$N(r) = N(qy - x) = |x - qy|^2 = |y|^2 \cdot \left|\frac{x}{y} - q\right|^2 < |y|^2 = N(y).$$

This shows that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.