FALL 2019: MATH 558 HOMEWORK

The page numbers in each assignment below refer to those in the course textbook. Turn in only the problems in bold face.

HW 1. Section 1.3: 1, 12, **14, 20, 22**, 24, and read Section 1.2. Due September 6.

HW 2. Section 1.3: **25**, 26, **29**. Due September 6.

HW 3. Define a relation on $\mathbb{Z}$ as follows: For all $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $a - b$ is divisible by 4. Prove that $\sim$ is an equivalence relation, and identify, with proof, the distinct equivalence classes. To be turned in on September 13.

HW 4. Section 1.3: **21**, and also describe the equivalences classes of the indicated equivalence relation. Due September 13.

HW 5. Section 2.3: 6, 8, **9, 10**. Due September 13.

HW 6. Section 2.3: **12** and the following problem. Use the Well Ordering Principle to prove the following statement: Every natural number is divisible by a prime number. Hint: Suppose the statement is false and apply the Well Ordering Principle to the set of integers for which the statement fails. This is a proof by contradiction. Both problems are to be turned in on September 13.

HW 7. Section 2.3: **15a, 15f**, 16, **17c**, 18, 19, **20**. Hint for **17c**: Let $a = \frac{1+\sqrt{5}}{2}$ and $b = \frac{1-\sqrt{5}}{2}$ and show that a, b are roots of $x^2 - x - 1$. From this, show that a, b satisfy $x^{n+1} = x^n + x^{n-1}$, for all $n \geq 1$ and then use induction on n to prove the required statement. Due September 20.

HW 8. Section 2.3: 17a, 17e, **22**, **28**, 29, **31**. Due September 20.

HW 9. Section 2.3: **21**. Due September 20.

HW 10. Read Section 17.2 and work Section 17.4: **4a, d**. Due September 27.

HW 11. Find the GCD of $f(x) = x^2 - 1$ and $g(x) = x^4 + 6x^3 + x + 1$ over $\mathbb{Q}[x]$ and write it as a polynomial combination of $f(x)$ and $g(x)$.

HW 12. Section 17.4: **17, 18.** And, the following problem, to be turned in: Use problem 17 to prove that if $p(x) \in F[x]$, and $a \in F$, then $p(a) = 0$ if and only if $x - a$ divides $p(x)$. Due October 4.

HW 13. Section 17.4: **21, 22**. Due October 4. Hint: For 21, try to mimic the standard proof showing the existence of infinitely many prime numbers.

HW 14. Write addition and multiplication tables for $\mathbb{Z}_6$. Write a multiplication table for the **non-zero** elements in $\mathbb{Z}_7$. Due October 18.

HW 15. Let R be an integral domain and let $R[x]$ denote the ring of polynomials with coefficients in R. Prove that $R[x]$ is an integral domain. Due October 18

HW 16. Section 16.6: **3a,b,c** and the following problem (to be turned in). Use the division algorithm in $\mathbb{Z}$ to find the multiplicative inverse of $\overline{83}$ in the field $\mathbb{Z}_{97}$. Due October 18.

HW 17. Due October 25. Let R denote the set of complex numbers of the form $a + b\sqrt{3}i$, with $a, b \in \mathbb{Z}$. Define $N : R \to \mathbb{Z}_{\geq 0}$, by $N(a + b\sqrt{3}i) = a^2 + 3b^2$. Prove:

(i) R is closed under addition and multiplication. Conclude R is a ring and also an integral domain.
(ii) Prove $N(xy) = N(x)N(y)$, for all $x, y \in R$.
(ii) Prove that $1, -1$ are the only units in R.

HW 18. Due October 25. 1. Let R be an integral domain. Define a relation on R by $a \sim b$ if and only if $a = bu$, for some unit u. Prove that $\sim$ is a equivalence relation and describe the resulting equivalence classes.

2. Suppose R is Euclidean domain, and d_1 and d_2 are greatest common divisors of the non-zero elements a and b. Prove that $v(d_1) = v(d_2)$. Due October 25.

HW 19. Due October 25. Let $\mathbb{Z}[i]$ denote the Gaussian integers, with norm $N(a + bi) = a^2 + b^2$. Recall that $\pm 1, \pm i$ are the only units i $\mathbb{Z}[i]$.

(i) Use the norm N to show that $1 + i$ is irreducible in $\mathbb{Z}[i]$.
(ii) Write 2 as a product of distinct irreducible elements in $\mathbb{Z}[i]$.

HW 20. Due November 1. In this assignment, we will see an example of an integral domain that has elements that can be factored as a product of irreducible elements, but that factorization is not unique. Let R denote the set of all complex numbers $a + b\sqrt{5}i$, where $a, b \in \mathbb{Z}$. Let N be the norm on R defined by $N(a + b\sqrt{5}i) = a^2 + 5b^2$. As before $N(z_1z_2) = N(z_1)N(z_2)$, for all $z_1, z_2 \in R$. (In fact, this holds for all complex numbers if, for $z = c + di \in \mathbb{C}$ we define $N(z) = c^2 + d^2$.)

(i) Show that R is an integral domain.
(ii) Show that the only units in R are ± 1.
(iii) Use the norm to prove that $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ are irreducible elements in R.
(iv) Conclude that $6 = 2 \cdot 3 = (1 + \sqrt{5}i) \cdot (1 - \sqrt{5}i)$ are two distinct factorizations of 4 into a product of irreducible elements.

HW 21. Due November 1. For Gaussian integers $z = 8 + 12i$ and $w = 2 + 3i$, write $z = wq + r$, with Gaussian integers w, r such that $r = 0$ or $N(r) < N(w)$.

HW 22. Due November 8. Prove that $L := \{a + b\sqrt{5}i \mid a, b \in \mathbb{Q}\}$ is a field containing the roots of $x^2 + 5$. Moreover, prove that if $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is a field containing the roots of $x^2 + 5$, then $L \subseteq K$.

HW 23. Due November 8. We are working with the roots of $p(x) = x^3 - 11$.

(i) Find the three roots of $p(x)$ (as complex numbers).
(ii) Show that the roots you found in (i) all have the form $\alpha \cdot \sqrt[3]{11}$, where α is one of the three cube roots of 1 and $\sqrt[3]{11}$ is the real cube root of 11.
(iii) Take the roots r_1, r_2, r_3 you found in part (i) and verify that $x^3 - 11 = (x - r_1)(x - r_2)(x - r_3)$.

HW 24. Due November 8. Recall from class that $\mathbb{Q}(\sqrt[3]{2})$ is the field consisting of all real numbers of the form $\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4}$, with $\alpha, \beta, \gamma \in \mathbb{Q}$. Let $a = 3 + 2\sqrt[3]{2} + \sqrt[3]{4}$ and $b = 1 + 5\sqrt[3]{4}$ belong to $\mathbb{Q}(\sqrt[3]{2})$. Calculate $a \cdot b$ and a^{-1} as elements of $\mathbb{Q}(\sqrt[3]{2})$.

HW 25. Due November 8. Let $\alpha \in \mathbb{C}$ be a root of $x^2 + x + 1 \in \mathbb{Q}[x]$. For $\gamma = 3 + 2\alpha \in \mathbb{Q}(\alpha)$, find γ^{-1} as an element of $\mathbb{Q}(\alpha)$.

HW 26. Due November 15. (i) Show $f(x) = 2x^3 + 6x^2 + 6$ is irreducible over $\mathbb{Q}$ and (ii) Find all roots of $g(x) = x^3 - 2x^2 - x - 6$.

HW 27. Due November 15. Fix $f(x) = x^2 + x + 1$, let R denote the ring $F[x]$ mod $f(x)$.

(i) Calculate $\overline{3 + 5x} + \overline{1 + 6x}$ and $\overline{3 + 5x} \cdot \overline{1 + 6x}$ in R.
(ii) Use what you did in HW 25 to find the multiplicative inverse of $\overline{3 + 2x}$ in R.

HW 28. Due November 22. (i) Let K denote the commutative ring $\mathbb{Z}_3[x]$ mod $x^2 + x + 2$. Write out addition and multiplication tables for K. Conclude that K is a field with nine elements that contains a root of $x^2 + x + 2$.

(ii). Let L denote the commutative ring $\mathbb{Z}_2[x]$ mod $x^3 + x + 1$. Write a multiplication table for the non-zero elements of L. Conclude that L is a field with eight elements containing a root of $x^3 + x + 1$.

HW 29. Due December 6.

1. Let $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ belong to S_3 (as in class). Use the relations derived in class (or the group table of S_3) to calculate $\sigma\tau^2\tau\sigma\tau^7\sigma^5\tau$.

2. Let $x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be elements in the group $\mathrm{Gl}_2(\mathbb{Z}_2)$. Verify the following relations:

(i) $x^3 = I$, $y^2 = I$.
(ii) $yx = x^2y$.

Do these three relations look familiar? Can you make a prediction about the group table for $\mathrm{Gl}_2(\mathbb{Z}_2)$ in light of what you know about the group table of S_3?

HW 30. Due December 6. Write out group tables for the following groups: (a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and (b) $\mathbb{Z}_2 \times \mathbb{Z}_4$. Note $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are abelian groups of order eight with $+$ as their binary operation. Do these groups seem the same to you, or is there something different about them?

HW 31. Due December 11. Here is an interesting group, called the *Quaternion group* and denoted by Q_8. We have $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where:

$$(-1)^2 = 1, i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j,$$

and multiplication by -1 is the the expected value and -1 commutes with all elements of Q_8.

(i) Write the group table for Q_8.
(ii) Show that $H := \{\pm 1\}$ and $K := \{\pm 1, \pm i\}$ are subgroups of Q_8.
(iii) Find the **distinct** left cosets of H and K.

HW 32. Due December 11.

1. For $G = S_3$, with our usual notation, let $H = \{I, \tau, \tau^2\}$ and $K = \{I, \sigma\}$. Find the distinct right cosets of H and K. How do the left cosets of H compare to the corresponding right cosets? How do the left cosets of K compare to the corresponding right cosets?

2. Repeat the steps in the previous problem for $G = Q_8$, and H and K described in Homework 31.