MATH 5320 - FINAL EXAM REVIEW PROBLEMS.

1) Is the ring $\mathbb{Z}/6\mathbb{Z}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$? Is the ring $\mathbb{Z}/8\mathbb{Z}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$? Justify your answers.

Solution: The first two rings are isomorphic by the Chinese Reminder Theorem. The ring $\mathbb{Z}/8\mathbb{Z}$ is not a a product of two rings since it has no non-trivial idempotents, check that.

2) Find the quotient $\mathbb{Z}^3/N$ (in the normal form) where N is a submodule generated by the columns of the matrix

$$\begin{pmatrix} 2 & 2 & 4 \\ 0 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}$$

Solution: Row-column reduction over $\mathbb{Z}$ gives

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Hence $\mathbb{Z}^3/N \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}$.

3) Using invertible row column operations over the ring $\mathbb{Z}[i]$, diagonalize into a normal form the matrix

$$\begin{pmatrix} 3 & 2+i \\ 2-i & 9 \end{pmatrix}$$

Solution: $3/(2+i) = 6/5 - 3/5i$ hence the closest gaussian integer is $1-i$. Thus $3 = (1-i)(2+i)+i$. Multiply the second column by $1-i$ and subtract it from the first,

$$\begin{pmatrix} i & 2+i \\ -7+8i & 9 \end{pmatrix}$$

$(-7+8i)/i = 8+7i$. Multiply the first row by $8+7i$ and subtract from the second,

$$\begin{pmatrix} i & 2+i \\ 0 & -22i \end{pmatrix}$$

$(2+i)/i = 1-2i$. Multiply the first column by $1-2i$ and subtract from the second,

$$\begin{pmatrix} i & 0 \\ 0 & -22i \end{pmatrix}.$$

4) Let $\zeta_9 = e^{2\pi i/9}$ be a primitive 9-th root of 1. Prove that $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$ i.e. find the minimal polynomial for ζ_9 and prove that it is irreducible.

Solution: $x^9 - 1 = (x^3-1)(x^6+x^3+1)$, so ζ_9 is a root of x^6+x^3+1. This polynomial is irreducible by Eisenstein criterion, after replacing x by $x+1$, check this.

5) Prove that $x^5 + 5x + 5$ is irreducible over $K = \mathbb{Q}(\zeta_9)$.

Solution: This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein criterion. Let α be a root of this polynomial. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Using the previous exercise, and that 5 and 6 are relatively prime, $[\mathbb{Q}(\alpha, \zeta_9) : \mathbb{Q}] = 30$, hence $[K(\alpha) : K] = 5$.

6) Find the minimal polynomial, over $\mathbb{Q}$, of $1+\alpha \in \mathbb{Q}(\alpha)$ where α is a root of $x^3 - 2x - 2 = 0$.

Solution: Substitute $x - 1$ for x.

7) Let $\omega = e^{\frac{2\pi i}{3}}$. Prove that the ring $\mathbb{Z}[\omega]$ is euclidean i.e. for every $\alpha, \beta \in \mathbb{Z}[\omega]$, with $\beta \neq 0$, show that there exists $\gamma, \delta \in \mathbb{Z}[\omega]$, such that $\alpha = \gamma\beta + \delta$, and $N(\delta) < N(\beta)$, where $N(\alpha) = \alpha\bar{\alpha}$.

8) Let F be a field of characteristic p where p is a prime. Prove that $\mathrm{Fr} : F \to F$ defined by $\mathrm{Fr}(x) = x^p$ is a homomorphism.

9) Let $p \neq 3$ be a prime and F a finite field of order p^2. Note that $p^2 \equiv 1 \pmod 3$. Let $g \in F^\times$ be a primitive element i.e. of order $p^2 - 1$. Let $\omega = g^{\frac{p^2-1}{3}}$. Prove that $s = \omega - \omega^2$ is a square root of -3. Compute $\mathrm{Fr}(s)$ to determine p such that $s \in \mathbb{F}_p$.

Solution: $s^2 = \omega^2 - 2\omega^3 + \omega^4 = \omega^2 - 2 + \omega = -3$ since $\omega^2 + \omega + 1 = 0$. (Any cube root of 1 different from 1 is a root of $x^2 + x + 1$.) $\mathrm{Fr}(s) = \omega^p - \omega^{2p}$ and this depends on p modulo 3. If p is 1 modulo 3 then $\mathrm{Fr}(s) = s$, otherwise $\mathrm{Fr}(s) = \omega^2 - \omega^4 = \omega^2 - \omega = -s$. Hence -3 is a square modulo p if and only if p is 1 modulo 3.

10) Let $\omega = e^{\frac{2\pi i}{3}}$. Use the previous problem to determine $p \neq 3$ such that $\mathbb{Z}[\omega]/(p)$ is a field, i.e. (p) is a maximal ideal in $\mathbb{Z}[\omega]$.

Solution: In fact we do not need the previous exercise. $\mathbb{Z}[\omega] \cong \mathbb{Z}[x](x^2 + x + 1)$ hence $\mathbb{Z}[\omega]/(p) \cong \mathbb{F}_p[x](x^2 + x + 1)$ and the latter is a field if and only if $\mathbb{F}_p$ does not contain cube roots of 1 i.e. p is congruent 2 modulo 3.

11) Compute the number of monic, irreducible polynomials of degree 6 in $\mathbb{F}_p[x]$.

Solution: A root of any such polynomial generates $\mathbb{F}_{p^6}$. An element of $\mathbb{F}_{p^6}$ either generates $\mathbb{F}_{p^6}$ or it is contained in subfields $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^2}$. These two fields intersect in $\mathbb{F}_p$. Thus the number of elements that generate $\mathbb{F}_{p^6}$ is $p^6 - p^3 - p^2 + p$. Divide by 6 to answer the question.